Exhibit 19

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ASKELADDEN L.L.C.,
Petitioner,

v.

VERIFY SMART CORP.,
Patent Owner.

Case IPR2017-______
Patent No. 8,285,648

PETITION FOR *INTER PARTES* REVIEW OF CLAIMS 1-19 OF U.S. PATENT NO. 8,285,648

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I. INTRODUCTION 1

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8(a)(1)..........................3

A. Real Party-In-Interest Under 37 C.F.R. §42.8(b)(1) 3

B. Related Matters Under 37 C.F.R. §42.8(b)(2) 3

C. Lead and Back-Up Counsel Under 37 C.F.R. §42.8(b)(3) 4

D. Service Information Under 37 C.F.R. §42.8(b)(4)...............................4

III. PAYMENT OF FEES UNDER 37 C.F.R. §42.103 4

IV. GROUNDS FOR STANDING UNDER 37 C.F.R. §42.104(a)......................5

V. IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. §42.104(b) AND RELIEF REQUESTED 5

A. Claims for Which *Inter Partes* Review Is Requested Under 37 C.F.R. §42.104(b)(1)...5

B. The Specific Art and Statutory Grounds on Which the Challenge Is Based Under 37 C.F.R. §42.104(b)(2) 5

VI. SUMMARY OF THE '648 PATENT 6

A. Specification of the '648 Patent 6

VII. CLAIM CONSTRUCTION UNDER 37 C.F.R. §42.104(b)(3) 8

A. "device identifier" 9

VIII. APPLICATION OF CITED PRIOR ART TO EVERY CLAIM FOR WHICH *INTER PARTES* REVIEW IS REQUESTED UNDER 37 C.F.R. §42.104(b)(4)-(5) 10

A. Level Of Ordinary Skill In The Art...10

B. Ground 1: Claims 1-15 and 19 Are Unpatentable Under 35 U.S.C. §103(a) as Obvious Over Law in view of Dua 10

1. The Disclosure of Law 11

2. The Disclosure of Dua 15

3. Obviousness of Claims 1-15 and 19 of the ’648 Patent 16

4. Claim Charts 25

A. Ground 2: Claims 16-18 Are Unpatentable Under 35 U.S.C. §103(a) as Obvious Over Law and Dua in View of Salveson 63

1. The Disclosure of Salveson 63

2. Obviousness of Claims 16-18 of the ’648 Patent 65

IX. CONCLUSION 71

TABLE OF AUTHORITIES

Page(s)

Cases

In re GPAC Inc.,
57 F.3d 1573 (Fed. Cir. 1995) 10

KSR Int'l Co. v. Teleflex Inc.,
550 U.S. 398 (2007)..*passim*

Okajima v. Bourdeau,
261 F.3d 1350 (Fed. Cir. 2001) 10

Statutes

35 U.S.C. §102(b) 5, 11, 15, 63

35 U.S.C. §103(a) 6, 10, 63

35 U.S.C. §§311-319...1

35 U.S.C. §315 5

Other Authorities

37 C.F.R. §42 1

37 C.F.R. §42.8(a)..3

37 C.F.R. §42.8(b) 3, 4

37 C.F.R. §42.10(a)..4

37 C.F.R. §42.10(b) 4

37 C.F.R. §42.15(a)..4

37 C.F.R. §42.100(b) 9

37 C.F.R. §42.103 4

37 C.F.R. §42.104(a)..5

37 C.F.R. §42.104(b) 5, 8, 10

37 C.F.R. §42.108 1

EXHIBIT LIST

EXHIBIT NO.	**DESCRIPTION**
1001	U.S. Patent No. 8,285,648 to Goodin ("the '648 Patent")
1002	Expert Declaration of Ivan Zatkovich in Support of Petition for *Inter Partes* Review of Claims 1-19 of U.S. Patent No. 8,285,648 ("Zatkovich Decl.")
1003	*Curriculum Vitae* of Ivan Zatkovich
1004	Prosecution History of U.S. Appl. No. 12/443,426
1005	US 2005/0184145 A1 to Law et al. ("Law")
1006	US 2006/0165060 A1 to Dua ("Dua")
1007	U.S. Patent No. 6,886,741 to Salveson ("Salveson")
1008	U.S. Patent Office Assignment Record for U.S. Patent No. 8,285,648
1009	*Verify Smart Corp. v. Ally Bank* Complaint for Patent Infringement
1010	Developing Wireless Applications using the Java 2 Platform, Micro Edition; Bill Day
1011	Understanding Logon and Authentication

Pursuant to 35 U.S.C. §§311-319 and 37 C.F.R. §42, Askeladden L.L.C. ("Petitioner") respectfully petitions for *Inter Partes* Review of Claims 1-19 of U.S. Patent No. 8,285,648 ("the '648 Patent," Ex.1001), which is believed to be currently assigned to Verify Smart Corp. ("Verify Smart" or "Patent Owner"). Petitioner submits the Expert Declaration of Ivan Zatkovich (Ex.1002) in support of this Petition. As demonstrated herein with the support of testimonial evidence, there is a reasonable likelihood that Petitioner will prevail in establishing that at least one of the challenged claims is unpatentable. Accordingly, institution of an IPR under 37 C.F.R. §42.108 is requested.

I. INTRODUCTION

The '648 Patent discloses and claims a system and method for verifying the identity of a user in a financial transaction. During an enrollment process, a user is assigned a PIN or password ("bona fide secure identifier"), which is stored in a "verifier-database" accessible to a "verifier-computer." (Ex.1001, 4:24-29, 6:52-55, Fig. 1). When the user wishes to execute a financial transaction such as a credit card purchase, the verifier-computer opens a communications link and sends an "identity verification request (IVR)" to the user's mobile device, which requests entry of the assigned PIN or password. (*Id*. at 4:34-41, 8:13-39). In response, the user enters and sends a "putative secure identifier" to the verifier-computer, which the verifier-computer compares to the previously assigned bona fide secure identifier. (*Id*. at 8:51-57). If they match, the financial transaction proceeds. (*Id*. at 9:5-10).

Law (Ex.1005) discloses the identical verification technique. Specifically, Law discloses a "real-time authorization" method in which a user initiates a transaction with a third party. (Ex.1005, ¶36). The transaction is put in a "pending" state while the third-party submits an authorization request to an "authorization server." (*Id*. at ¶47). The server then sends an authorization request to the user's wireless device with the transaction details. (*Id*. at ¶¶47, 49, 56-57). Just like in the '648 Patent, the user authorizes the transaction by entering a PIN number, which is transmitted back to the authorization server. (*Id*. at ¶49). If the PIN provided is correct, the authorization server allows the transaction to proceed. (*Id*. at ¶50).

The remaining claim elements of then '648 Patent were trivial and obvious to a person of ordinary skill in the art at the relevant time, and expressly disclosed by Dua (Ex.1006) and Salveson (Ex.1007). As discussed below, Dua and Salveson are directed to the same field of endeavor as Law—electronic transaction processing—and a POSITA would have been motivated to combine their respective teachings.

Thus, there is a reasonable likelihood that Petitioner will prevail in establishing that at least one of Claims 1-19 of the '648 Patent is unpatentable over the prior art.

II. MANDATORY NOTICES UNDER 37 C.F.R. §42.8(a)(1)

As set forth below and pursuant to 37 C.F.R. §42.8(a)(1), the following mandatory notices are provided as part of this Petition.

A. Real Party-In-Interest Under 37 C.F.R. §42.8(b)(1)

Petitioner, Askeladden L.L.C., is the real party-in-interest.

B. Related Matters Under 37 C.F.R. §42.8(b)(2)

The Patent Office Assignment Database shows that the ’648 Patent is shown as assigned to Dan Scammell (*see* Ex.1008), but Verify Smart asserts in its patent infringement complaints that the patent is currently assigned to Verify Smart (*see, e.g.*, Ex.1009, *Verify Smart Corp. v. Ally Bank,* Complaint,¶6).

To date, Verify Smart has filed eighteen patent infringement lawsuits in various district courts in Texas, New Jersey and New York. Lawsuits against the following parties are currently pending:

- First Republic Bank (NYSD-1-16-cv-09078),
- Valley National Bancorp (NJD-2-16-cv-06065) and
- Discover Financial Services (NJD-2-16-cv-08647).

None of the defendants in those cases is a real party in interest or a privy of Petitioner in this proceeding.

In addition, petitions filed by Bank of America, NA, (CBM2015-00173) and

Unified Patents Inc. (IPR2016-00836) were each dismissed before an institution decision.

C. Lead and Back-Up Counsel Under 37 C.F.R. §42.8(b)(3)

Pursuant to 37 C.F.R. §§42.8(b)(3) and 42.10(a), Petitioner provides the following designation of lead and back-up counsel and related service information. Pursuant to 37 C.F.R. §42.10(b), a Power of Attorney accompanies this Petition.

Lead Counsel	Back-Up Counsel
Charles R. Macedo (Reg. No. 32,781) Amster, Rothstein & Ebenstein LLP 90 Park Avenue New York, NY 10016 Telephone: (212) 336-8074 Facsimile: (212) 336-8001 E-mail: cmacedo@arelaw.com	Mark Berkowitz (Reg. No. 64,558) Amster, Rothstein & Ebenstein LLP 90 Park Avenue New York, NY 10016 Telephone: (212) 336-8063 Facsimile: (212) 336-8001 E-mail: mberkowitz@arelaw.com

D. Service Information Under 37 C.F.R. §42.8(b)(4)

Service information (by e-mail, postal mailing, or hand-delivery) for lead and back-up counsel is provided in the above designation of lead and back-up counsel. Petitioner also consents to electronic service by e-mail at PQI-VS-IPR@arelaw.com, with a copy to cmacedo@arelaw.com.

III. PAYMENT OF FEES UNDER 37 C.F.R. §42.103

The undersigned hereby provides authorization to charge Deposit Account No. 01-1785 to cover the $24,600 fee for this Petition. 37 C.F.R. §42.15(a). If this amount is insufficient or excessive, the Commissioner is authorized to deduct any underpayment from, or credit any overpayment to, Account No. 01-1785.

IV. GROUNDS FOR STANDING UNDER 37 C.F.R. §42.104(a)

Petitioner certifies that: (1) the ’648 Patent is available for *Inter Partes* Review and (2) the provisions of 35 U.S.C. §§315(a), 315(b), and 315(e)(1) do not bar or estop Petitioner from requesting *inter partes* review of Claims 1-19 of the ’648 Patent on the grounds raised herein.

V. IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. §42.104(b) AND RELIEF REQUESTED

A. Claims for Which *Inter Partes* Review Is Requested Under 37 C.F.R. §42.104(b)(1)

Petitioner requests *Inter Partes* Review of Claims 1-19 of the ‘648 Patent.

B. The Specific Art and Statutory Grounds on Which the Challenge Is Based Under 37 C.F.R. §42.104(b)(2)

This Petition for *Inter Partes* Review is based on the following prior art:

(1) U.S. 2005/0184145 A1 to Law et al. (“Law,” Ex.1005), which was published on August 25, 2005, and is prior art under 35 U.S.C. §102(b).

(2) U.S. 2006/0165060 A1 to Dua (“Dua,” Ex.1006), which was published on July 27, 2006, and is prior art under 35 U.S.C. §102(b).

(3) U.S. Patent No. 6,886,741 to Salveson (“Salveson,” Ex.1007), which issued on May 3, 2005 and is prior art under 35 U.S.C. §102(b).

This Petition requests cancellation of Claims 1-19 of the ’648 Patent based on the following specific grounds:

Ground 1: Claims 1-15 and 19 are unpatentable under 35 U.S.C. §103(a) as obvious over Law in view of Dua; and

Ground 2: Claims 16-18 are unpatentable under 35 U.S.C. §103(a) as obvious over Law and Dua in view of Salveson.

VI. SUMMARY OF THE ’648 PATENT

The ’648 Patent, entitled “System and Method for Verifying a User’s Identity in Electronic Transactions,” issued on October 9, 2012.

The application that matured into the ’648 Patent was a PCT application (PCT/CA2007/001639) filed in Canada on September 14, 2007, which entered the U.S. national phase (as Appl. No. 12/443,426) on March 27, 2009. Thus, for the purpose of this Petition, the priority date of the ’648 Patent is September 14, 2007.

A. Specification of the ’648 Patent

The ’648 Patent is generally directed to methods for verifying the identity of a user during an electronic transaction. The patent notes that credit card transactions are often subject to fraudulent activity and present additional security problems. (Ex.1001, 2:60-3:9). The patent further asserts that these problems are often ignored, as a matter of convenience. (*Id.* at 3:6-9). Thus, it asserts that, “[w]hat is needed is a method of and system for verifying the identity of a user during an electronic-transaction wherein the method is easy to implement, easy to use, and substantially transparent to the user …” (*Id.* at 3:52-57).

The ’648 Patent describes using a verification code to verify the identity of a user in a financial transaction. During an enrollment process, a user is assigned a PIN or password (“bona fide secure identifier”), which is stored in a “verifier-database” accessible to a “verifier-computer.” (*Id.* at 4:24-29, 6:52-55, Fig. 1). The user’s mobile device is also associated with the user’s account. (*Id.* at 6:60-7:14). A “flag” is placed in the user’s account to indicate that transactions must be verified by the user before allowing to proceed. (*Id.* at 7:15-32). The steps of the enrollment process are shown in Figure 1 of the ’648 Patent (reproduced below).

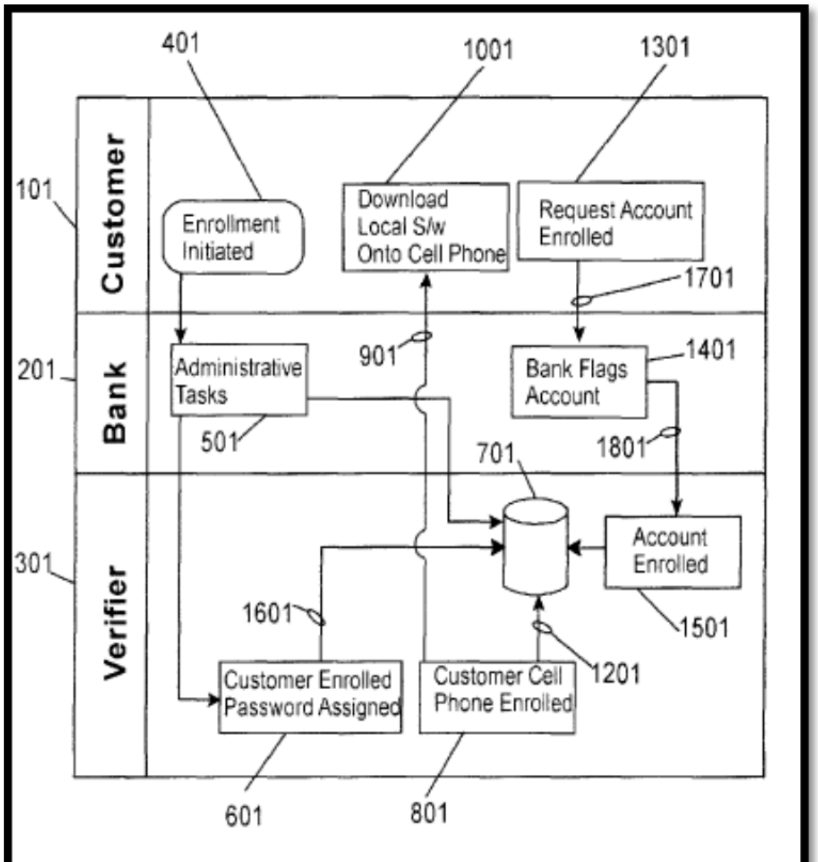


Fig 1

When the user wishes to execute a financial transaction, such as a credit card purchase, the verifier-computer opens a communications link and sends an "(IVR)" to the user's mobile device, which requests entry of the assigned PIN or password. (*Id*. at 4:34-41, 8:13-39). In response, the user enters and sends a PIN or password ("putative secure identifier"), which the verifier-computer compares to the previously assigned bona fide secure identifier. (*Id*. at 8:51-57). If they match, the financial transaction is allowed to proceed. (*Id*. at 9:5-10). A flowchart of the verification process is shown in Figure 2 of the '648 Patent (reproduced below).

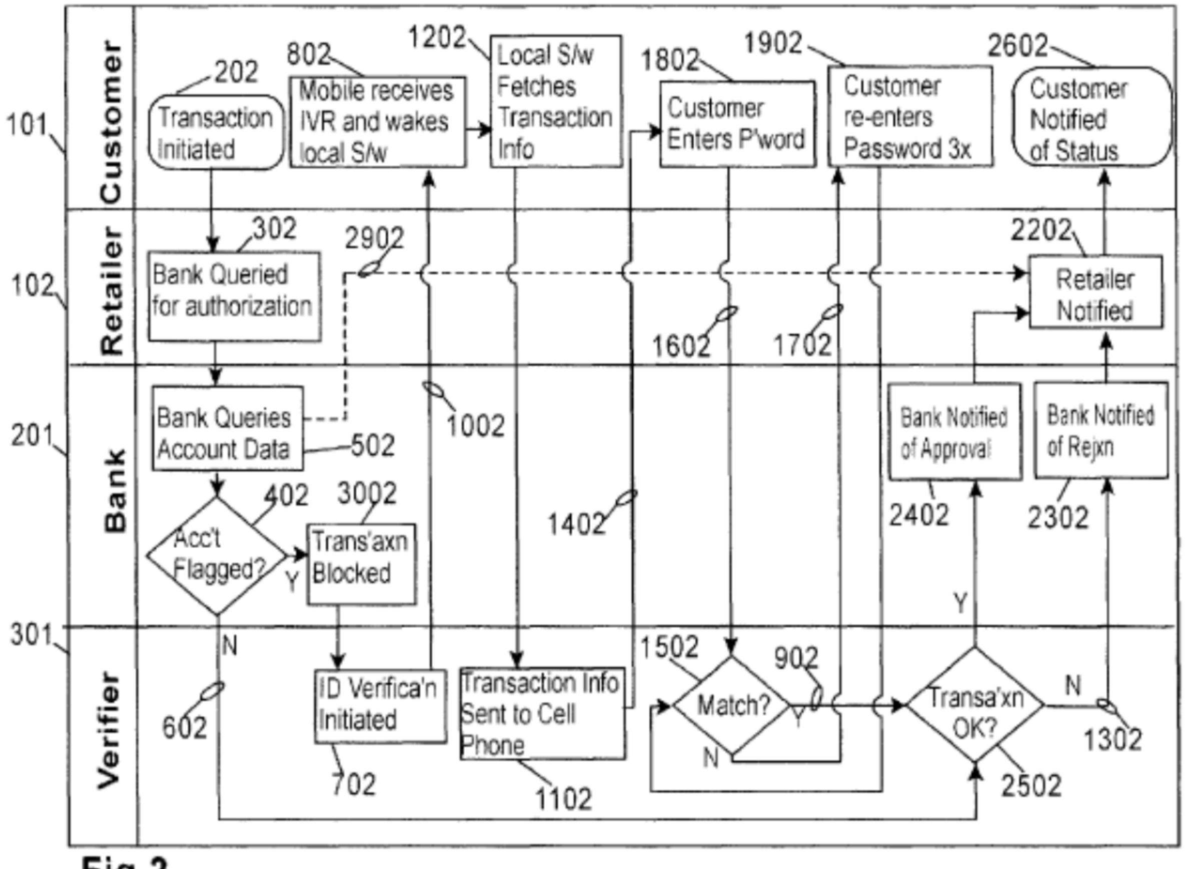


Fig 2

VII. CLAIM CONSTRUCTION UNDER 37 C.F.R. §42.104(b)(3)

Petitioner submits that, for purposes of this Petition only, most of the terms of the claims of the ’648 Patent are clear on their face, and should be given their broadest reasonable construction in light of the specification of the ’648 Patent. 37 C.F.R. §42.100(b).

Patent Owner has defined various terms in the Background of the ’648 Patent. (Ex.1001, 1:10–2:55). Petitioner adopts those definitions for purposes of this Petition.

The following additional claim term is construed based on the broadest reasonable construction:

A. “device identifier”

The ’648 Patent doesn’t use the term “device identifier” outside the claims, except in “Statement 15,” which was added during prosecution and merely repeats Claim 19. (Ex.1001, 18:5–15). However, “device identification information” is described:

> “At this point the verifier can optionally also acquire from the mobile phone a device identification information that can be used to identify that particular phone. In embodiments in which the user–computer is a laptop computer, PDA, or other computer instead of a mobile communications device, the serial number of the computer’s CPU can be acquired by the verifier.”

(Ex.1001, 7:6–13). Consistent with this use, Petitioner submits the construction of “device identifier” is *device identification information that can be used to identify* *a particular device, including alphanumeric representations such as CPU serial numbers, device keys, certificates, SIM numbers, IMEI numbers, or phone numbers.* (Ex.1002, ¶40).

VIII. APPLICATION OF CITED PRIOR ART TO EVERY CLAIM FOR WHICH *INTER PARTES* REVIEW IS REQUESTED UNDER 37 C.F.R. §42.104(b)(4)-(5)

A. Level Of Ordinary Skill In The Art

For purposes of the obviousness analyses presented below, Petitioner submits that the level of ordinary skill in the art is reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc*., 57 F.3d 1573, 1579 (Fed. Cir. 1995).

To the extent necessary to define further, Petitioner asserts that a POSITA for the ’648 Patent in the relevant field in 2007 would have a bachelor’s degree in computer science or a related study and two years of experience with electronic transactions and user authentication methods or the equivalent. (Ex.1002, ¶43).

B. Ground 1: Claims 1-15 and 19 Are Unpatentable Under 35 U.S.C. §103(a) as Obvious Over Law in view of Dua

As discussed below, Law and Dua teach each and every element of Claims 1-15 and 19, either expressly or inherently, and/or each of these elements would have been obvious to a POSITA at the time that the ’648 Patent was filed. (Ex.1002, ¶44).

1. The Disclosure of Law

Law, entitled "Secure Wireless Authorization System," was published on August 25, 2005 and is therefore prior art under 35 U.S.C. §102(b). The USPTO did not consider Law during the prosecution of the '648 Patent.

Law discloses "a secure wireless authorization system by which a user can employ a wireless device to authorize a request that is initiated by a remote third party and transmitted to the user by an authorization server." (Ex.1005, Abstract). Law describes three authorization models that can be implemented with the disclosed system: pre-authorization, real-time authorization and post-authorization. (*Id*. at ¶42).

Of particular relevance here is the real–time authorization model shown in Figure 3 (reproduced below), in which the identity of a user is authenticated during a financial transaction. (*Id*. at ¶47, Fig. 3). Like the claimed invention of the '648 Patent (Ex.1001, 9:55–57), the real-time authorization model disclosed by Law (Fig. 3 or 6) can be used to verify the identity of a buyer in a financial transaction. (Ex.1005 at ¶21).

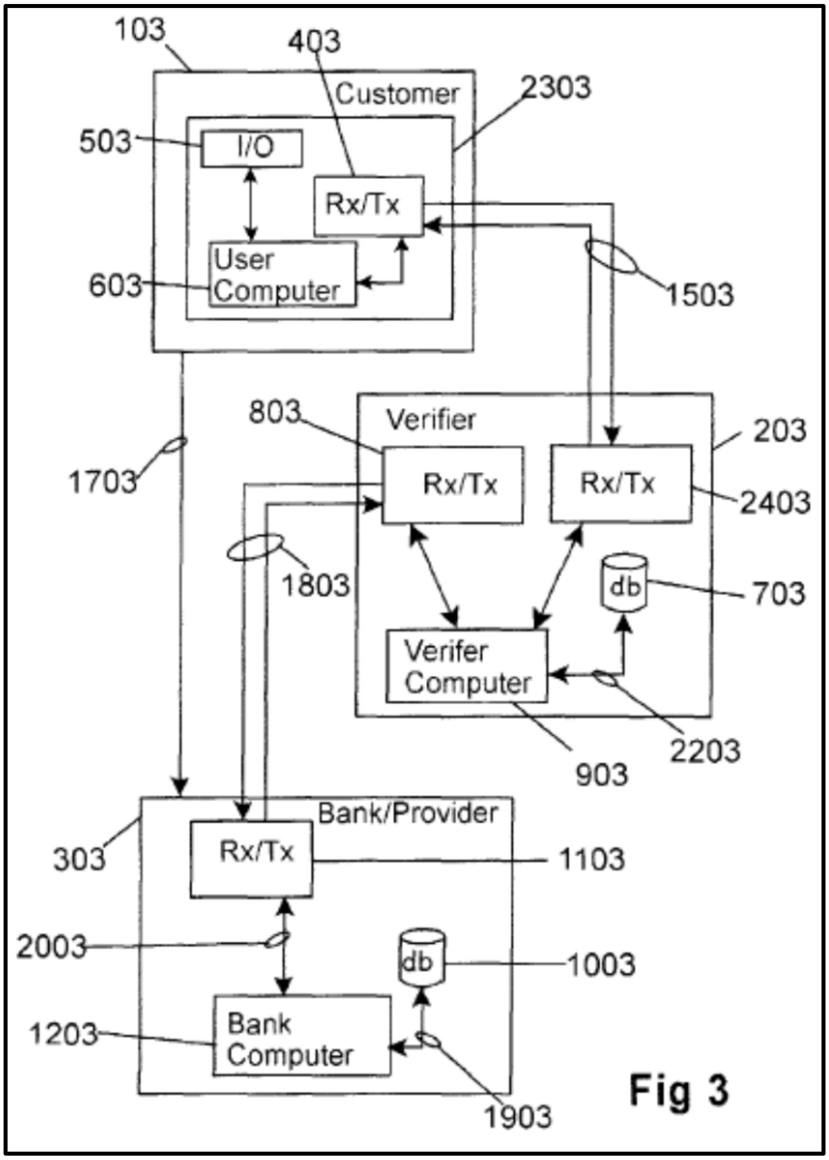


Fig 3

In this real-time authorization model, a user initiates a transaction with a third party. (Ex.1005, ¶36). The transaction is put in a "pending" state while the third-party submits an authorization request to an "authorization server." (*Id.* at ¶47). The server then sends an authorization request to the user's wireless device with the transaction details. (*Id.* at ¶¶47, 49, 56-57). "A message similar to 'company X requests action Y for an amount Z, would you like to proceed?' would be displayed on the wireless device." (*Id.* at ¶49).

The user authorizes the transaction by entering a PIN number, which is transmitted back to the authorization server. (*Id.* at ¶49). If the PIN provided is correct, the authorization server sends a response back to the third party to allow the transaction to proceed. (*Id.* at ¶50). *See* Fig. 6 reproduced below.

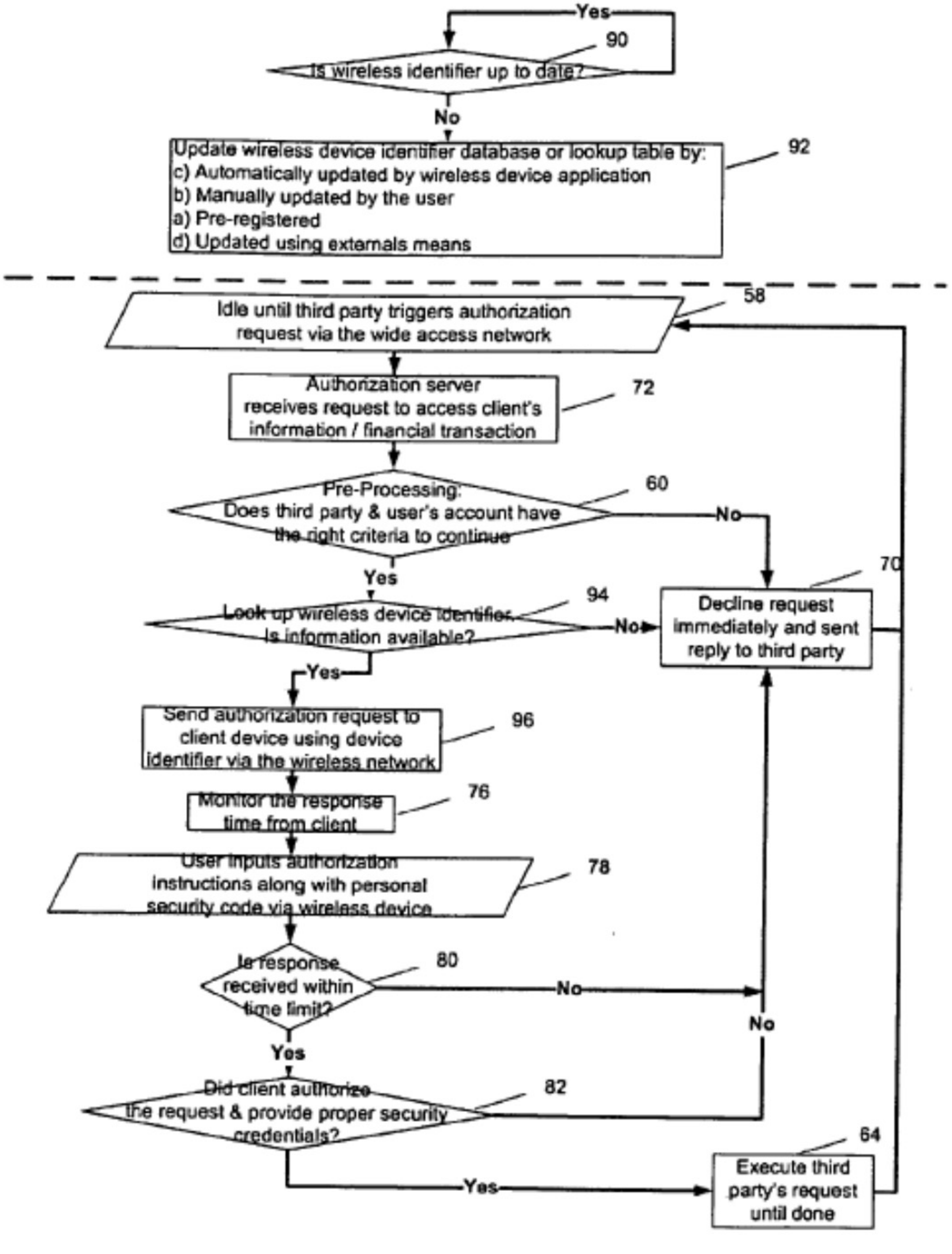

Yes
90
Is wireless identifier up to date?
No
Update wireless device identifier database or lookup table by:
c) Automatically updated by wireless device application
b) Manually updated by the user
a) Pre-registered
d) Updated using externals means
92
Idle until third party triggers authorization request via the wide access network
58
Authorization server receives request to access client's information / financial transaction
72
Pre-Processing: Does third party & user's account have the right criteria to continue
60
No
Yes
70
Look up wireless device identifier. Is information available?
94
No
Decline request immediately and sent reply to third party
Yes
Send authorization request to client device using device identifier via the wireless network
96
Monitor the response time from client
76
User inputs authorization instructions along with personal security code via wireless device
78
Is response received within time limit?
80
No
No
Yes
Did client authorize the request & provide proper security credentials?
82
Yes
64
Execute third party's request until done

FIG. 6

2. The Disclosure of Dua

Dua, entitled "Method and Apparatus for Managing Credentials Through a Wireless Network," discloses methods and devices for conducting financial and other transactions using a wireless device. (Ex.1006, Cover, Abstract). Dua, was published on July 27, 2006, and is prior art under 35 U.S.C. §102(b).

Dua recognizes that "consumers typically carry multiple single-purpose cards, tags, passes …" (*Id.* at ¶3). Dua also notes that various solutions to this issue have been proposed, such as "electronic wallet software" residing on a wireless device. (*Id.* at ¶18). According to Dua, the "primary hurdle to the broad-based deployment of such a solution is the difficulty in providing for the convenient, efficient, and secure distribution of credentials into wireless devices such that only those authorized to conduct the transaction may do so and only to the extent of their authorization." (*Id.*).

In connection with this problem, Dua discloses a "system and method through which credential issuers can securely and rapidly target specific wireless devices for the distribution of the appropriate credentials over public and private networks." (*Id.* at ¶¶20, 38). Of relevance here, Dua utilizes a wallet application downloaded onto the user's wireless device. (*Id.* at ¶199). This application may be downloaded "over the air" to the user's wireless device, during the registration process. (*Id.*). Also of relevance, Dua teaches verifying financial transactions using a PIN. (*Id*. at ¶366, 398).

3. Obviousness of Claims 1-15 and 19 of the ’648 Patent

Claims 1-15 and 19 are unpatentable as obvious over Law in view of Dua. As discussed below, it would have been obvious to a POSITA to combine the teachings of Law and Dua. Law and Dua are both in the same field of endeavor, i.e., directed to electronic transaction processing and, in particular, verifying and authenticating users and authorizing financial transactions. (Ex.1002, ¶54).

a. <u>It Would Have Been Obvious to “Pre-Enroll” Users in Law’s System</u>

Law discloses an authentication system that is virtually identical to that disclosed and claimed in the ’648 Patent. However, Law does not explicitly discuss every detail necessary to implement the disclosed system. This is because a POSITA would understand that certain elements or steps must be included in order to construct a working system. (Ex.1002, ¶55).

Independent Claim 1 recites the step of “pre-enrolling the user,” which further includes “assigning to the user a bona fide secure identifier” and “storing the bona fide secure identifier in a database that is accessible to the verifier.” Independent Claim 5 does not use the term “pre-enrolling,” but includes similar steps of “assigning a bona fide secure identifier to the user” and “storing the bona fide secure identifier of Step (a) in a database that is accessible to the verifier.” (*Id*. at ¶56).

At the time of the alleged invention, a POSITA would understand that, absent these pre-enrollment steps, it would not be possible for Law to perform the disclosed comparison at the time of verification. (*Id*. at ¶57). Indeed, the ’648 Patent provides little detail regarding pre-enrollment of a user, presumably because this was a well-known practice, and is consistent with the state of the art at the time of the alleged invention. (*Id*.). In all events, Dua explicitly discloses the step of pre-enrolling a user in an authentication/authorization system. (Ex. 1002, ¶57). Specifically, Dua teaches generating a PIN and mailing it to the user of the disclosed electronic wallet application. (*Id.*). Therefore, as Mr. Zatkovich testifies, in view of the teachings of Dua, it would have been obvious to a POSITA to pre-enroll a user in the system of Law. (*Id.*).

With respect to the "assigning" step, Law describes a real-time authorization process that verifies a user by comparing information obtained from a user with information stored in a database. (*See, e.g.*, Ex.1005, ¶63 ("Upon receiving the response [e.g., PIN] from the wireless device, the authorization server will check if the response was received within a specified timeout period (Block 80) and verify the security credentials…"), and ¶58). A POSITA would understand that this information would need to be assigned by an issuing bank (or selected by the user) and stored in a database. (Ex.1002, ¶58). This practice existed long before the priority date of the ‘648 Patent and would have been obvious to a POSITA, as confirmed by Dua, which expressly discloses a "credential issuance process" for an electronic wallet in which a financial institution "generate[s] a personal identification number (PIN) which may be mailed to the customer." (Ex.1006, ¶58; *see also id.* at ¶180). Thus, it would have been obvious to a POSITA to implement Dua's credential issuance process in Law's system to assign the PIN to a user. (Ex.1002, ¶59).

With respect to the "storing" step, Law discloses a database that is accessible to the authorization server 24 of the issuing bank. Law explains that the mobile devices GUID is "pre-registered" and stored in a database accessible to the authorization server. (*See, e.g.,* Law ¶60 ("For ***GUIDs*** that rarely change, such as SMS numbers, they can be pre-registered …")). As Mr. Zatkovich explains, a POSITA would understand that this database stores user account information, which necessarily includes the PIN (bona fide secure identifier). (Ex.1002, ¶60). This is because a PIN (or other secure identifier) must be stored in the database for the comparison. (*See, e.g.*, Law ¶¶49-50). Furthermore, under *KSR*, "if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *KSR Int'l Co. v. Teleflex Inc.,* 550 U.S. 398, 417 (2007). Therefore, at a minimum, it would have been obvious to a POSITA, working at the time of the invention, to implement the system disclosed by Law by using a pre-registered PIN and GUID stored in the database, to provide an effective implementation. (Ex.1002, ¶60).

b. "Downloading Local Software" to a "Communication Device" Was Well-Known to a POSITA

Dependent Claims 7-11 depend, either directly or indirectly, from Claim 5 and further require "downloading local software to the user communications device." Similarly, Law discloses that the "wireless device must also be able to store an application that will process the request from the authorization." (Ex.1005, ¶41). This application "will be responsible for setting up the secure connection 32, securely storing certificates/encryption keys, displaying the request, accepting and creating the response." (*Id.*). However, Law does not explicitly state when and how this application is installed or loaded onto the wireless device. However, a POSITA would have known how to download local software to a wireless device. (Ex.1002, ¶61).

In this regard, at the time of the filing of the '648 Patent, there were three predominant methods for loading software onto a wireless device. The software could be loaded onto the device: (1) at the time of manufacture; (2) through a physical connection; or (3) over a wireless connection. (Ex.1002, ¶62). As Mr. Zatkovich explains, standards for performing these methods would have been well known by a POSITA. (*Id.* (discussing Ex.1010, 6-7)).

Where there are only a “finite number of identified, predictable solutions,” it would have been “obvious [to a POSITA] to try” each of these options. *See KSR,* 550 U.S. at 421. In this case, a POSITA would have selected the technique most suited to their design requirements. (Ex.1002, ¶63). Furthermore, Dua expressly discloses downloading software to be stored on handsets over the air. (Ex.1006, ¶199). As was well-known at the time, this method of software delivery is convenient. (Ex.1002, ¶64). In addition, this method allows for the software to be readily updated in the future. (*Id.*). Thus, it would have been an obvious design choice to download software as taught in Dua for implementing the system of Law. (*Id.*).

Dependent Claim 8 further requires that “the IVR sent at Step (f) [of Claim 5] includes the bona fide secure identifier retrieved at Step (j) [of Claim 5].” Here too, in implementing the system of Law with the local software of Dua, a POSITA would have been presented with a limited number of known options. As above, where there are only a “finite number of identified, predictable solutions,” it would have been “obvious [to a POSITA] to try” each of these options. *KSR,* 550 U.S. at 421. Specifically, a POSITA would have understood that the bona fide secure identifier could be sent along with the verification request or, alternatively, sent at an earlier point in time. (Ex.1002, ¶65). Thus, it would have been obvious to a

POSITA to include the bona fide secure identifier in the IVR to improve system efficiency. (*Id.*).

c. <u>**The Prior Art Taught That The Verification Could Be Performed On The Authentication Server Or By The Local Software**</u>

Claim 8 further requires that the local software perform the step of comparing the putative secure identifier (input by the user) with the bona fide secure identifier (retrieved from the database). As a practical matter, a POSITA implementing the system of Law would have been faced with just two options to perform the comparison: (1) on the server side; or (2) on the client side. (*Id*. at ¶66). Thus, here too, there were just a finite number of identified, predictable solutions available to a POSITA. (*Id*.). A POSITA at the time of the invention would understand that performing the comparison on the server side is more secure than performing the comparison on the client side. (*Id*. at ¶67). By contrast, a POSITA at the time of the invention would understand that performing the comparison on the client side would be a more efficient. (Ex.1002, ¶68, citing Ex.1011, 31).

Dua confirms that the above options were known in the art, since it recognizes that PINs may be verified on the server side or "offline" by the mobile device. (Ex.1011, ¶398; *see also id.* at ¶399). In order to build an efficient system, a POSITA would have been motivated by Dua to modify Law to have the comparison to occur at the at the wireless device. (Ex.1002, ¶69).

d. **<u>"Transaction Authorization" Is Taught by Law and Dua</u>**

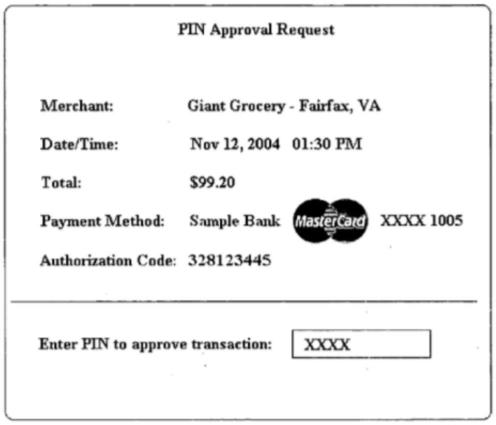
Independent Claim 5 recites steps for verifying a user's identity using an IVR. Dependent Claims 13 and 14 further require "authorizing the transaction." In this regard, the '648 Patent explains that identification verification can be performed simultaneously with, or independent of, the "transaction authorization". (*See, e.g.,* Ex.1001, 9:24-35). Law teaches that these two steps may be performed using a single message: "A message similar to 'company X requests action Y for an amount Z, would you like to proceed?' would be displayed on the wireless device." (Ex.1005, ¶49). The user then has an opportunity to respond to this message by entering his/her secure identifier on the wireless device to verify his/her identity and authorizes the transaction. (*Id.*). This disclosure satisfies both the user verification steps of Claim 5 and the transaction authorization steps of Claims 13-14. (Ex.1002, ¶70).

To the extent that Patent Owner argues that Claims 13-14 require sending a separate message to authorize the transaction, these claims would still be invalid as obvious. A POSITA would understand that, as taught in Dua, two discrete steps could be required:

1) a user must, first, verify their identity by entering a PIN to access the wallet application. (Ex.1006, ¶410).

2) separately, a transaction authorization is sent to the user's mobile device (*id.* at ¶411).

This is shown in Figure 9 below:



PIN Approval Request

Merchant: Giant Grocery - Fairfax, VA

Date/Time: Nov 12, 2004 01:30 PM

Total: $99.20

Payment Method: Sample Bank XXXX 1005

Authorization Code: 328123445

Enter PIN to approve transaction: XXXX

FIG. 9

(Ex.1002, ¶71).

Dua, thus, confirms that it was known that a user's identity and a transaction could be separately verified. (Ex.1002, ¶72). Dua explains the purpose of this two-step process is to provide the user with an additional opportunity to confirm and approve the transaction. (Ex.1006, ¶411). Therefore, a POSITA seeking to provide a user with an additional opportunity to review a transaction would have known that separate messages, as taught by Dua, could be used to: verify a user's identity and authorize a transaction. (Ex.1002, ¶72). Thus, a POSITA would consider it obvious to use a two-step method as taught in Dua in the system of Law so as to provide the user with an additional opportunity to confirm and approve the transaction. (*Id.*).

e. **<u>Setting A "Flag" In A Database Was Known to a POSITA and Taught By Dua</u>**

Claims 14 and 15 require setting a "flag" in a database. The flag indicates whether the user authentication steps should be performed, or whether the transaction may proceed without authentication. Law does not explicitly disclose setting such a flag in the database. Dua does show this limitation as necessary for Claims 14 and 15, which explicitly disclose placing a flag in a database record to indicate whether a transaction should proceed. (*Id*. at ¶73).

As for Claims 14-15, it would have been obvious to a POSITA to use a flag, which, as Dua confirms, was a common technique for conveying status in databases. (*Id*. at ¶74). The flag, as described in the '648 Patent as well as Dua, is a Boolean value. (*Id.*). Indeed, flags are one of the most basic elements in computer science. (*Id.*). Boolean values (i.e., true/false) have long been used to signify whether certain features are enabled, including those used within an account profile. (*Id.*).

Dua confirms that using a flag is an obvious design choice and one of a limited number of solutions to the problem of indicating that a transaction should be prevented from proceeding until the transaction has been verified by the user. (*Id*. at ¶75). Furthermore, Law explains that, prior to performing the authorization process, certain pre-authorization steps may be performed. (Ex.1005, ¶45). A POSITA would have understood at the time of the alleged invention that, before or after these steps, a flag could be checked to determine whether the user authorization should be performed. (Ex.1002, ¶75). Thus, a POSITA would consider it obvious to use a flag as taught in Dua in the system of Law, as a matter of design choice in computer programming. (*Id.*); *see also KSR,* 550 U.S. at 415-16 ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.").

4. Claim Charts

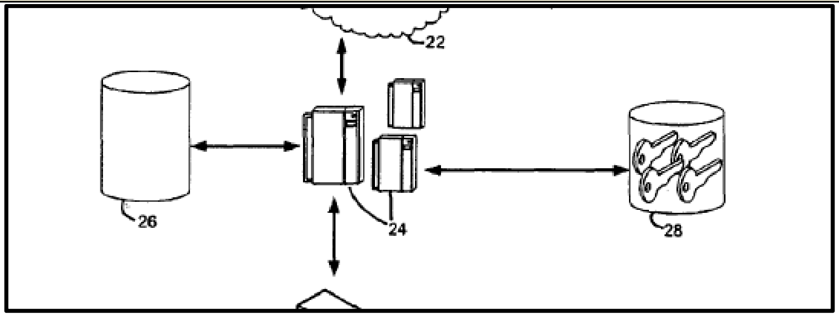
As shown in the Claim Charts below, Law and Dua combine to teach all the elements of Claims 1-15 and 19. As discussed above, there was a clear motivation to combine the references and a POSITA would have had a reasonable expectation of success when making this combination. As such Claims 1-15 and 19 are obvious over the teachings of Law and Dua. (Ex.1002, ¶76).

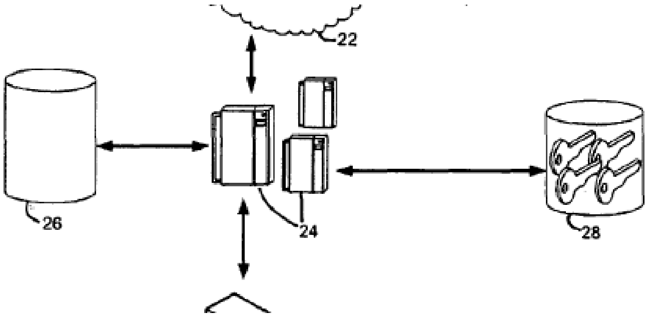
The '648 Patent	**Law and Dua**
1. A user identity verification method for verifying the identity of a user by a verifier in the course of an electronic transaction, said user identity verification method comprising the	**Law provides a user identity verification method ("real-time authorization protocol") for verifying the identity of a user by a verifier ("issuing bank") in the course of an electronic transaction.** Law ¶23 ("... ***The authorization server determines if the user and the third party have the right criteria.... the authorization server sends out an authorization request to the user's wireless device. The user either approves or denies the request along with a personal***

The '648 Patent	**Law and Dua**
steps of:	***identification number (PIN) or personal digital signature."***); *Id.* at ¶36 ("For example, ***the third party entity can be an online merchant 12 requesting authorization of a credit card transaction from the issuing bank. The request will be initiated by the online merchant, sent through the credit card network 22 and into the authorization server 24 of the issuing bank.***); Fig. 1.
(a) pre-enrolling the user, comprising the steps of:	**Law describes an authorization process which verifies a user by drawing upon and verifying already stored user information. As discussed above (§VIII.B.3.a), it would have been obvious to a POSITA in light of Law and Dua to "pre-enroll" the user prior to performing the verification method in order to perform the verification method described in Law.** Law ¶20 ("***Further, a database is linked to the authorization server to retain user information***."); Law ¶49 ("The user will have the opportunity to input the response through the wireless device and be able to provide a PIN or personal digital signature (Block 78)."); *Id.* at ¶63 ("Upon receiving the response from the wireless device, the authorization server will check if the response was received within a specified timeout period (Block 80) and verify the security credentials of the user and the wireless device (Block 82)."). **Dua explicitly discloses the pre-enrolling of a user, by generating a PIN and sending it to the user via mail.** Dua, ¶58 ("…***For example, the file may contain data indicating a request of the Personalization Bureau to generate a personal identification number (PIN) which***

The '648 Patent	**Law and Dua**
	may be mailed to the customer."); *Id.* at ¶180 ("…***The issuer could also request a special code or PIN that was mailed to the user in advance of the issuance as a means to further validate identity and ensure non-repudiation....***").
(a1) assigning to the user a bona fide secure identifier; and,	**Law describes an authorization process which verifies a user by drawing upon and verifying already stored user information. It would have been obvious to a POSITA to assign to the user a bona fide secure identifier, in view of the teachings of Law, Dua, and the knowledge of a POSITA. As discussed above (§VIII.B.3.a), a POSITA would understand that, in order for Law's verification method to function, a user would have to be assigned a secure identifier (e.g., a PIN or password) beforehand.** Law ¶20 ("***Further, a database is linked to the authorization server to retain user information***."); *Id.* at ¶66 ("The user will also enter ***a PIN*** to authenticate himself or herself to the authorization server"); *Id.* at ¶49 ("The user will have the opportunity to input the response through the wireless device and be able to provide a ***PIN or personal digital signature*** (Block 78)."); *Id.* at ¶63 ("Upon receiving the response from the wireless device, the authorization server will check if the response was received within a specified timeout period (Block 80) and ***verify the security credentials of the user*** and the wireless device (Block 82)."). **Dua explicitly discloses assigning to the user a bona fide secure identifier, by generating a PIN and mailing it to the user.**

The '648 Patent	**Law and Dua**
	Dua ¶58 ("***For example, the file may contain data indicating a request of the Personalization Bureau to generate a personal identification number (PIN) which may be mailed to the customer.***"); *Id.* at ¶180 ("… ***The issuer could also request a special code or PIN that was mailed to the user in advance of the issuance as a means to further validate identity and ensure non-repudiation…*** .").
(a2) storing the bona fide secure identifier in a database that is accessible to the verifier;	**Law describes an authorization process which verifies a user by drawing upon and verifying already stored user information. It would have been obvious to a POSITA at the time of the alleged invention to store the bona fide secure identifier in a database that is accessible to the verifier, in view of the teachings of Law and the knowledge of a POSITA. As discussed above (§VIII.B.3.a), a POSITA would understand that, in order for Law's authentication process to function, the secure identifier (e.g., a PIN or password) would have to be stored in a database that is accessible to the verifier.** Law ¶20 ("***Further, a database is linked to the authorization server to retain user information.***"); Law ¶63 ("Upon receiving the response from the wireless device, the authorization server will… ***verify the security credentials of the user*** and the wireless device (Block 82)."). **Fig. 1 shows that authorization server 24 is connected to database 26:**

The ’648 Patent	**Law and Dua**
	 **The authorization server 24 is described as later verifying a user (“W’s”) PIN, thus confirming the PIN is stored in database 26 along with other user information:** Law ¶44 (“The ***authorization server*** will verify the user W’s ***PIN*** and other security credentials (Block 54).”);
(b) pre-enrolling a user communications device, wherein pre-enrolling the user communications device comprises the steps of:	**Law discloses pre-enrolling (“pre-register[ing]”) a user communications device (“wireless device”).** Law ¶38 (“The authorization server 24 … is responsible for executing the required logic and procedure to ***obtain secure authorization from a user and his wireless device.***”); *Id.* at ¶39 (“Depending on which authorization model used, the server must keep track of ***the global unique identifier (GUID) of the wireless device*** in order to be able to contact it.”); ¶60 (“For ***GUIDs*** that rarely change, ***such as SMS numbers***, they ***can be pre-registered*** … .”); ¶65 (“[B]efore the authorization begins, ***the user registers*** its GUID with the authorization server (the “verifier”)).
(b1) obtaining a user access number for the user communications device, wherein the user access number can be used to open a communications link	**Law discloses the step of obtaining a user access number (a “GUID”, such as SMS numbers) for the user communications device (“wireless device”), wherein the user access number (“GUID”) can be used to open a communications link (“secure channel”) with the user communications device.**

The '648 Patent	**Law and Dua**
with the user communications device; and,	Law ¶39 ("…the server must keep track of ***the global unique identifier (GUID) of the wireless device in order to be able to contact it.***"); *Id.* at ¶60 ("For ***GUIDs*** that rarely change, ***such as SMS numbers***, they can be pre-registered … ."); *Id.* at ¶62 ("The [authorization] request will travel ***through an encrypted secure channel via wireless network 36 connecting the authorization server 24 and the user's wireless device 38***.").
(b2) storing the user access number in a database that is accessible to the verifier;	**Law discloses that the user access number ("GUID") is stored in a database that is accessible to the verifier (e.g., "issuing bank").** Law ¶39 ("The ***authorization server 24 includes a database 26 which stores the account information*** of the users they serve… . Depending on which authorization model used, the ***server must also keep track of the global unique identifier (GUID)*** of the wireless device in order to be able to contact it."). **Fig. 1 shows that authorization server 24 is operatively connected to database 26:**  *See also id.* at ¶60.
(c) retrieving the user access number stored at Step (b2);	**Law discloses retrieving ("look[ing] up") the user access number ("GUID") stored at Step (b2).** Law, ¶62 ("However, if no valid pre-authorization exists,

The '648 Patent	**Law and Dua**
	the ***authorization server will look up the GUID of wireless device 38*** and attempt to connect to the wireless device with the GUID obtained (Block 94).”).
(d) opening a communications link between the verifier and the user communications device by using the user access number retrieved at Step (c);	**Law discloses opening a communications link (“secure channel”) between the verifier (e.g., “issuing bank”) and the user communications device (the “wireless device”) by using the user access number (“GUID”) retrieved at Step (c).** Law ¶62 (“However, if no valid pre-authorization exists, ***the authorization server will look up the GUID of wireless device 38 and attempt to connect to the wireless device with the GUID obtained*** (Block 94).”).
(e) sending an identity verification request (IVR) from the verifier to the user through the communications link opened at Step (d);	**Law discloses sending an IVR (“an authorization request”) from the verifier (the “issuing bank”) to the user (“the user's wireless device”) through the communications link (“secure channel”) opened at Step (d).** Law ¶49 (“However if no valid pre-authorization exists, ***the server will send out an authorization request to the user's wireless device****….* ***The request will travel through an encrypted secure channel connecting the authorization server and the user's wireless device…***”).
(f) inputting by the user a putative secure identifier;	**Law discloses the user inputting a putative secure identifier (e.g., “a PIN”).** Law, ¶49 (“***The user will have the opportunity to input the response through the wireless device and be able to provide a PIN or personal digital signature*** (Block 78).”).
(g) sending through the communications link opened at Step (d) a response to the IVR of Step (e);	**Law discloses sending through the communications link (the “secure channel”) opened at Step (d) a response (e.g., “PIN”) to the IVR of Step (e).** Law, ¶40 (“The wireless device can also use SMS to return the message back to the authorization server….”);

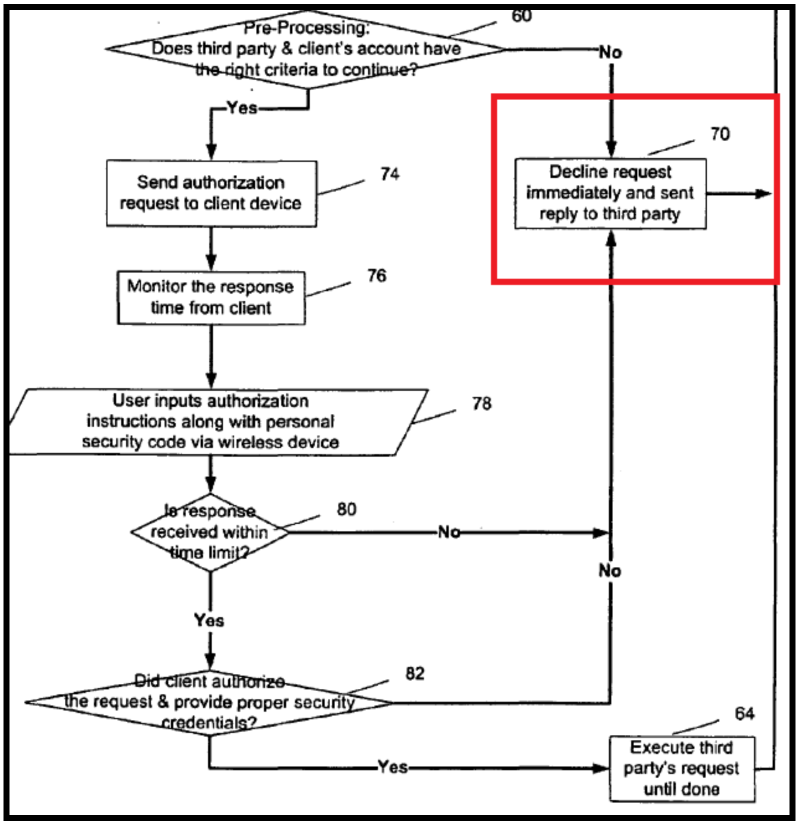
The '648 Patent	Law and Dua
	Id. at ¶49 ("***The PIN or digital signature along with the appropriate response parameters are sent back to the authorization server through an encrypted secure channel via the wireless network.***").
(h) retrieving the bona fide secure identifier stored at Step (a2);	**Law discloses retrieving the bona fide secure identifier (e.g., PIN) stored at Step (a2).** **Law discloses verifying the user's PIN ("secure identifier") with the one stored in the authorization server. A POSITA would understand that, since the user's PIN ("putative secure identifier") is compared to the PIN originally stored in Step (a2) (the "bona fide secure identifier"), the bona fide secure identifier ("PIN") stored at Step (a2) has necessarily been retrieved. (See Ex. 1002, p. 41).** Law ¶50 ("Upon receiving the response from the wireless device, ***the authorization server 24 will check if the response was received within a specified timeout period (Block 80) and verify the security credentials of the user and the wireless device*** (Block 82)…. If the correct security credentials are provided the specified instructions within the user's response will be executed by the authorization server."); *Id*. at ¶49 ("***The PIN*** or digital signature along with the appropriate response parameters are ***sent back to the authorization server*** through an encrypted secure channel via the wireless network."); *See also id*. ¶58-59.
(i) comparing the putative secure identifier input at Step (f) with the bona fide secure identifier	**Law discloses comparing ("verifying") the putative secure identifier (e.g., "PIN" sent back by user) supplied at Step (f) with the bona fide secure identifier (e.g., "PIN" stored in database) retrieved at Step (h).**

The '648 Patent	**Law and Dua**
retrieved at Step (h); and,	Law ¶49 ("***The PIN or digital signature along with the appropriate response parameters are sent back to the authorization server*** through an encrypted secure channel via the wireless network."); *Id.* at ¶50 ("***Upon receiving the response from the wireless device, the authorization server 24 will … verify the security credentials of the user and the wireless device*** (Block 82)."); *Id.* at ¶58 ("***The PIN or digital signature along with the appropriate response parameters are sent back to the authorization server 24 through an encrypted secure channel via the secure wireless network 36.***"); *Id.* at ¶59 ("Upon receiving the response from the wireless device 38, ***the authorization server*** *will …* ***verify the security credentials of the user*** and the wireless device (Block 82)").
(j) allowing the transaction to proceed only if the comparison of Step (i) results in a match between the putative secure identifier and the bona fide secure identifier.	**Law discloses allowing the transaction to proceed only if the comparison of Step (i) results in a match between the putative secure identifier ("PIN" entered by the user) and the bona fide secure identifier ("PIN" stored in the database).** Law ¶50 ("***If the correct security credentials are provided, the specified instructions within the user's response will be executed by the authorization server.*** An appropriate response will be sent back to the third party (Block 64)."); *Id.* at ¶47 ("This will allow the user to receive instant notification and provide time critical instructions to either authorize or deny the third party's request… ***The approval response will be processed by the authorization server and the appropriate actions taken.*** ");

<table>
<tr><th>The ’648 Patent</th><th>Law and Dua</th></tr>
<tr><td></td><td>

As shown in Figure 3 of Law below, if the correct security credentials are not provided as shown in box 82 (and there is no match between the putative secure identifier and the bona fide secure identifier), the request is declined and a reply is sent to the third party as shown in box 70.

Fig. 3:


Pre-Processing:
Does third party & client's account have the right criteria to continue?
60
No
Yes
70
Decline request immediately and sent reply to third party
Send authorization request to client device
74
Monitor the response time from client
76
User inputs authorization instructions along with personal security code via wireless device
78
Is response received within time limit?
80
No
No
Yes
Did client authorize the request & provide proper security credentials?
82
64
Execute third party's request until done
Yes

</td></tr>
<tr><td>

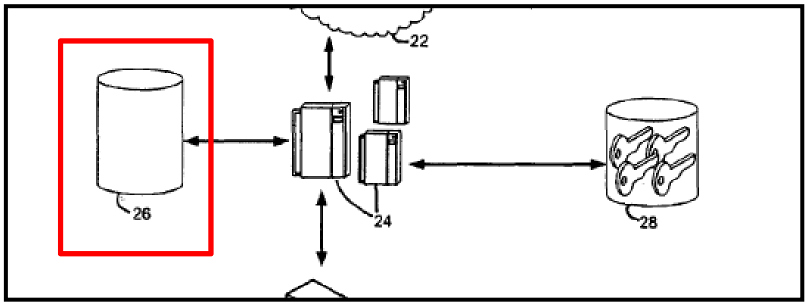
2. A system for verifying the identity of a user by a verifier during the course of an electronic transaction, said system comprising:

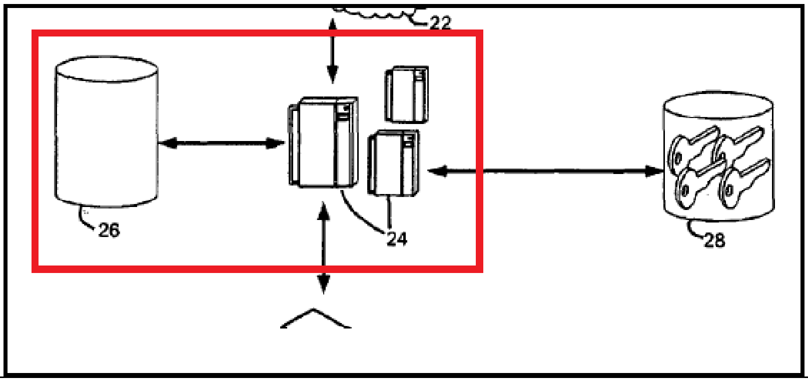
</td><td>

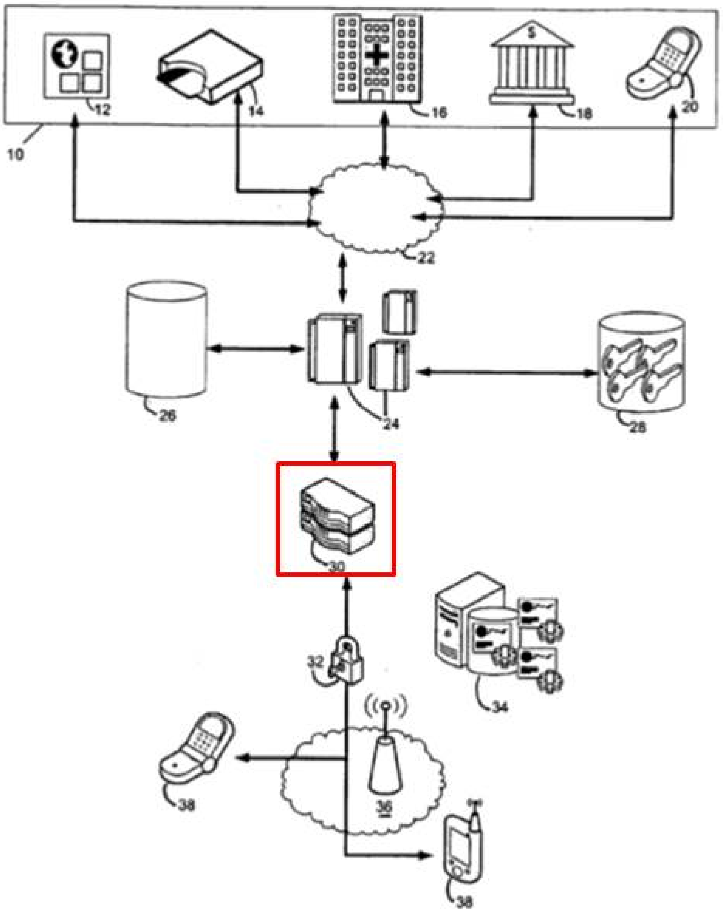
Law discloses a system for verifying the identity of a user by a verifier (e.g., “issuing bank”) during the course of an electronic transaction (e.g., credit card purchase).

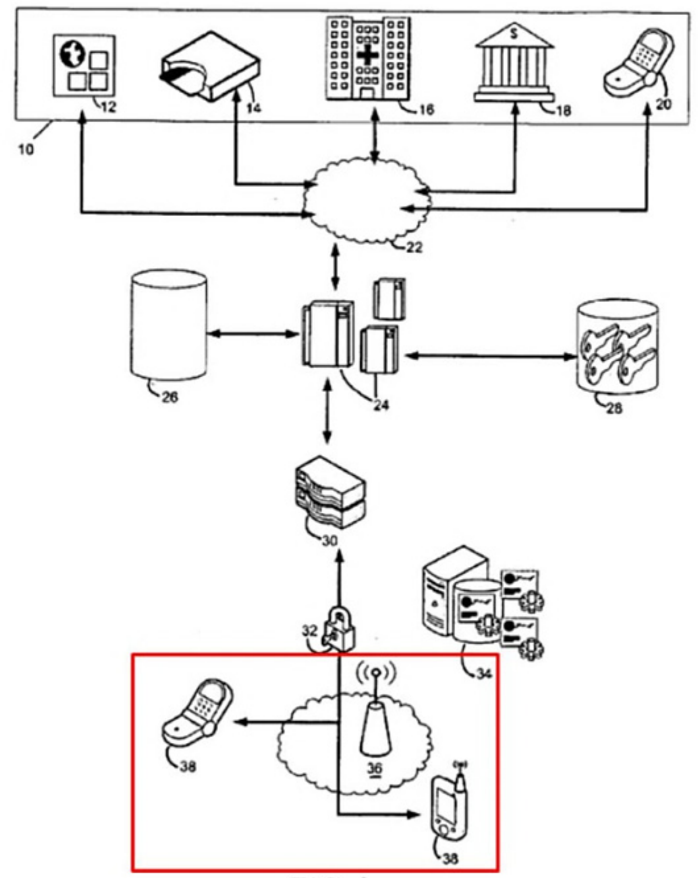
Law ¶36 (“… ***For example, the third party entity can be an online merchant 12 requesting authorization of a credit card transaction from the issuing bank. The request will be initiated by the online merchant, sent***

</td></tr>
</table>

<u>The ’648 Patent</u>	<u>Law and Dua</u>
	through the credit card network 22 and into the authorization server 24 of the issuing bank.”); *Id.* at ¶23 (“The real-time authorization model …. ***The transaction is placed in a pending state until the third party initiates a transaction request to the authorization server. The authorization server determines if the user and the third party have the right criteria…. the authorization server sends out an authorization request to the user’s wireless device.*** The user either approves or denies the request along with a personal identification number (PIN) or personal digital signature.”); Fig. 1.
a. a verifier-database (703);	**Law discloses a verifier-database (“database” which is operatively connected to the “authorization server”).** Law ¶20 (“Further, a database is linked to the authorization server to retain user information.”); ¶39 (“***The authorization server 24 includes a database 26 which stores the account information of the users they serve.***”). **Fig. 1 shows that authorization server 24 is operatively connected to database 26:** 
b. a verifier-computer (903), wherein said verifier-computer is adapted to write data to and retrieve data	**Law discloses a verifier-computer (the “authorization server 24”), wherein said verifier-computer is adapted to write data to and retrieve data (e.g., “account information”) from said verifier-database (“database 26”).**

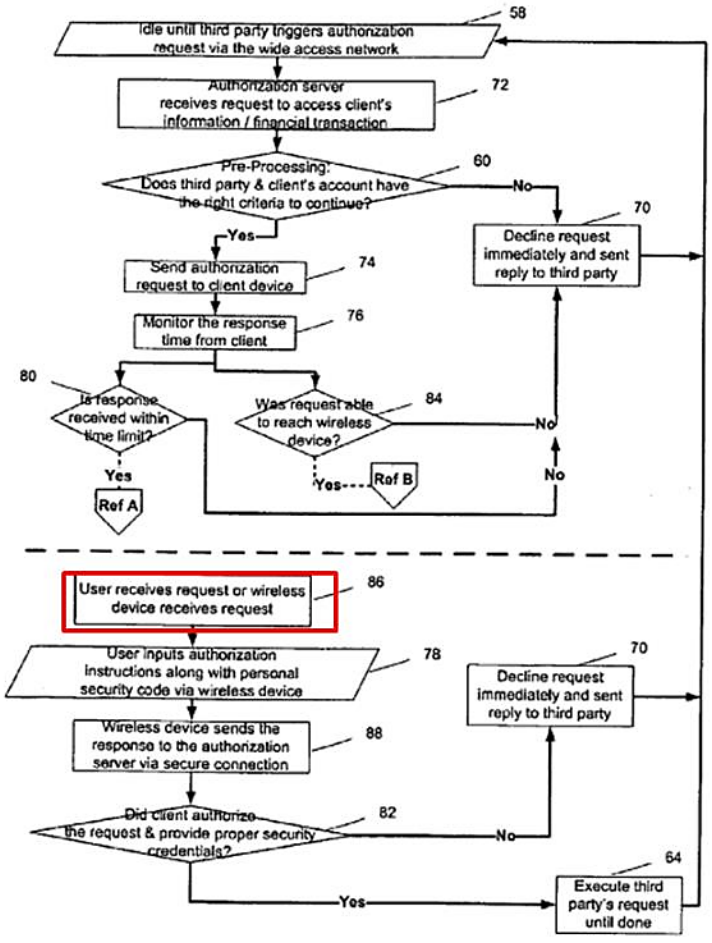
The '648 Patent	**Law and Dua**
from said verifier-database;	Law, ¶39 (***"The authorization server 24 includes a database 26 which stores the account information of the users they serve."***); *Id.* at ¶38 ("The authorization server 24 described herein is the central processing entity of the system. … In addition, it is also responsible for executing the third party request if and when the user does authorize the request."); **FIG. 1 shows that authorization server 24 is operatively connected to database 26:** 
c. a first verifier communications device (2403) for receiving communications from the user and transmitting communications to the user, wherein said first verifier communications device is accessible to said verifier-computer;	**Law discloses a first verifier communications device ("wireless gateway 30") for receiving communications from the user and transmitting communications to the user, and is accessible to said verifier-computer ("authorization server 24").** Law, ¶40 ("The **wireless gateway 30** is an entity that bridges the authorization server with the wireless network 36. It translates communication requests and information onto wireless network protocols that can be relayed to the wireless device."). **Fig. 1 shows that wireless gateway 30 is operatively connected to authorization server 24:**

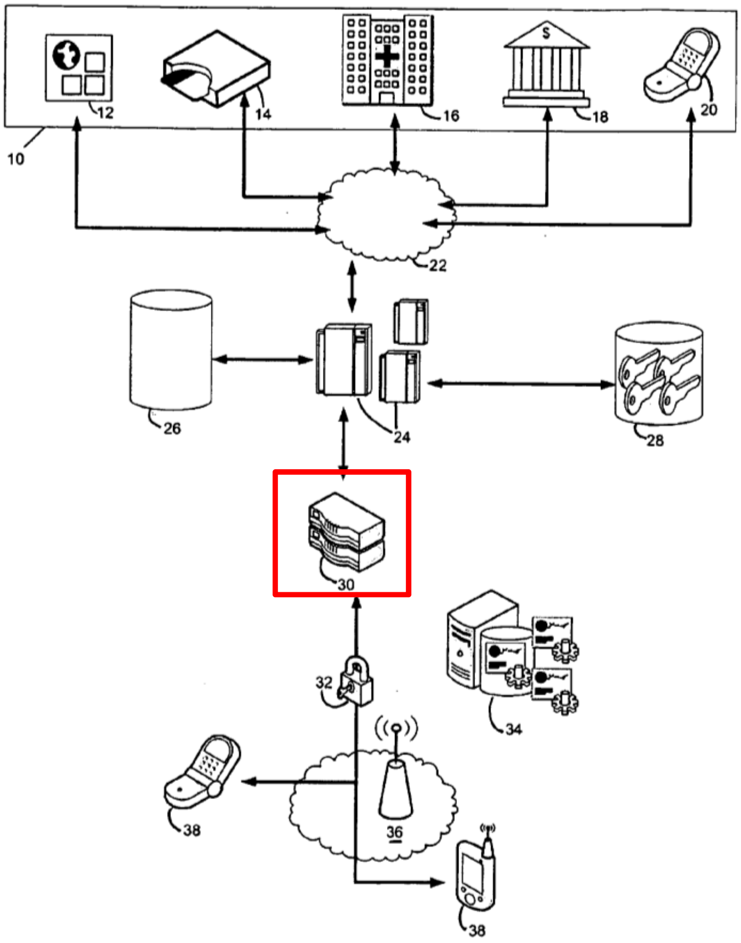
The ’648 Patent	**Law and Dua**
	 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 38 38 FIG. 1
d. a user communications device (2303) for receiving communications from the verifier and transmitting communications to the verifier, wherein said user communications device is accessible to the user;	**Law discloses a user communications device (“wireless device 38”) for receiving communications from the verifier and transmitting communications to the verifier (e.g., issuer bank) wherein the user communication device is accessible to the user.** Law, ¶41 (“The ***wireless device 38 is an entity which has the ability to notify users of authorization requests*** and ***also provide an interface for the user to respond to the authorization request***…. ***The wireless device must also be able to store an application that will process the request from the authorization server***…”); **Fig. 1 shows that wireless device 38 is operatively**

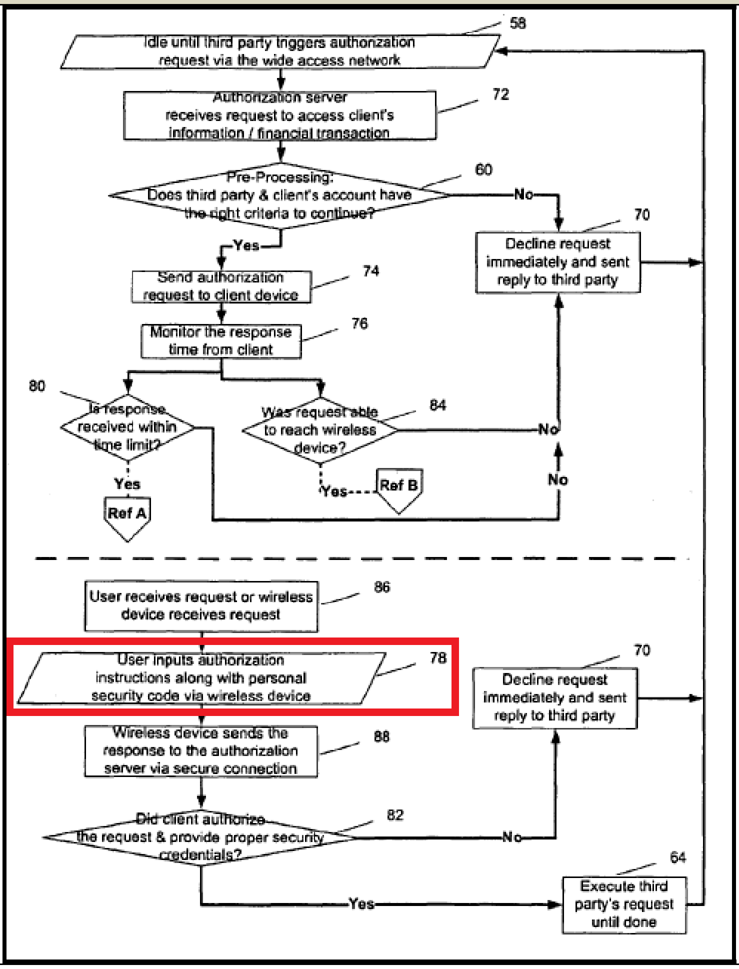
<u>**The ’648 Patent**</u>	<u>**Law and Dua**</u>
	connected to the authorization server 24 via wireless network 36.  12 14 16 18 20 10 22 26 24 28 30 32 34 38 36 38 FIG. 1
e. an input/output (I/O) (503) device that accepts input from the user and displays output to the user; and,	**Law discloses an input/output (I/O) device that accepts input from the user and displays output to the user. Specifically, a POSITA would understand, at the time of the alleged invention, that the communication device (e.g., wireless device 38) must include an input device (e.g., a physical or virtual keypad or keyboard, biometric sensor) in order to allow the user to input a secure identifier and access the “interface for the user to respond to the authorization request”. (Law** ¶41). **Likewise, a POSITA would understand that the communication device must include an output device (e.g., alphanumeric or graphical display the “interface”) to present information to the user. In this**

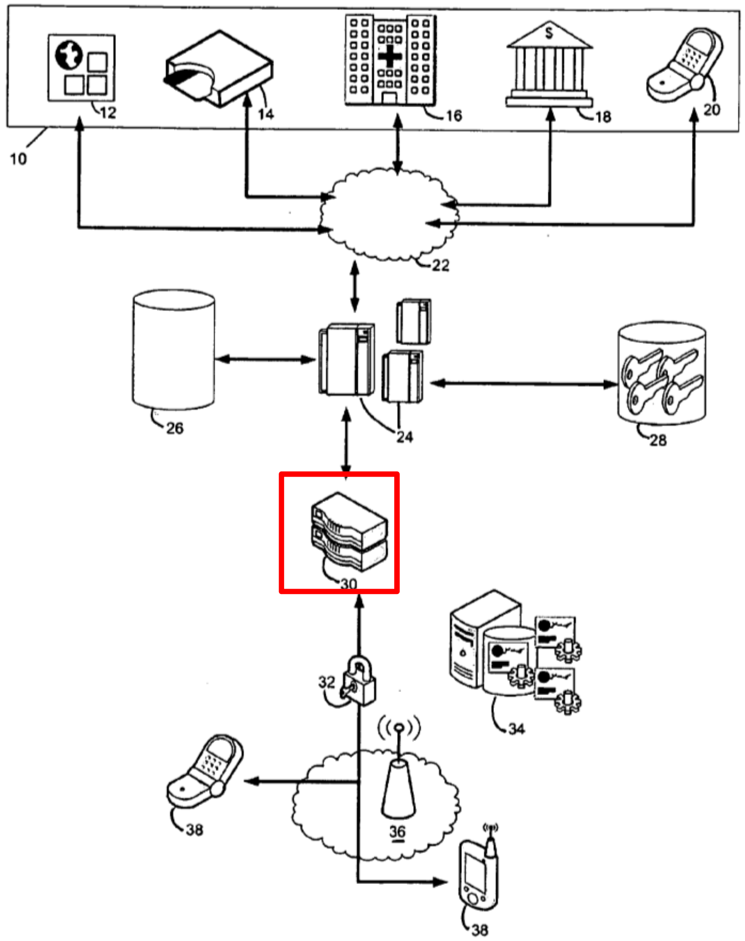
The '648 Patent	**Law and Dua**
	regard, input/output devices were a common feature of mobile devices at the time that the '648 Patent was filed. It would also be clear to a POSITA from the teachings of Law that Law's wireless device 38 included a means for notifying a user of a verification request and inputting a response in order for the user to "have the opportunity to input the response through the wireless device". (Law ¶63**).** Law ¶63 ("***Upon receiving the request, the wireless device 38 will notify the user and automatically display the request for the user. The user will have the opportunity to input the response through the wireless device and be able to provide a PIN or personal digital signature (Block 78***)."); ¶41 ("The ***wireless device 38*** ... also provide ***an interface for the user*** to respond to the authorization request.").
f. a user-computer (603) coupled to said user communication device and coupled to said I/O device, wherein said user-computer is adapted to:	**Law discloses a user-computer ("computationally capable" device) coupled to the user communication device and coupled to the I/O device.** **Specifically, a POSITA would understand that Law's wireless device 38 includes a user-computer (e.g., processor and memory) coupled to the device's input (e.g., keypad) and output (e.g., display). In this regard, at the time of the alleged invention, all mobile devices, including "smart phones" as specifically divulged in Law, include some form of processor or primary controller and memory. Law also specifically states that wireless device 38 "must be computationally capable of creating an encrypted secure connection," which would inform a POSITA that wireless device 38 includes a sophisticated computer.** Law ¶41 ("***The wireless device 38 must be computationally capable of creating an encrypted secure connection within a reasonable time.*** ... Typically the

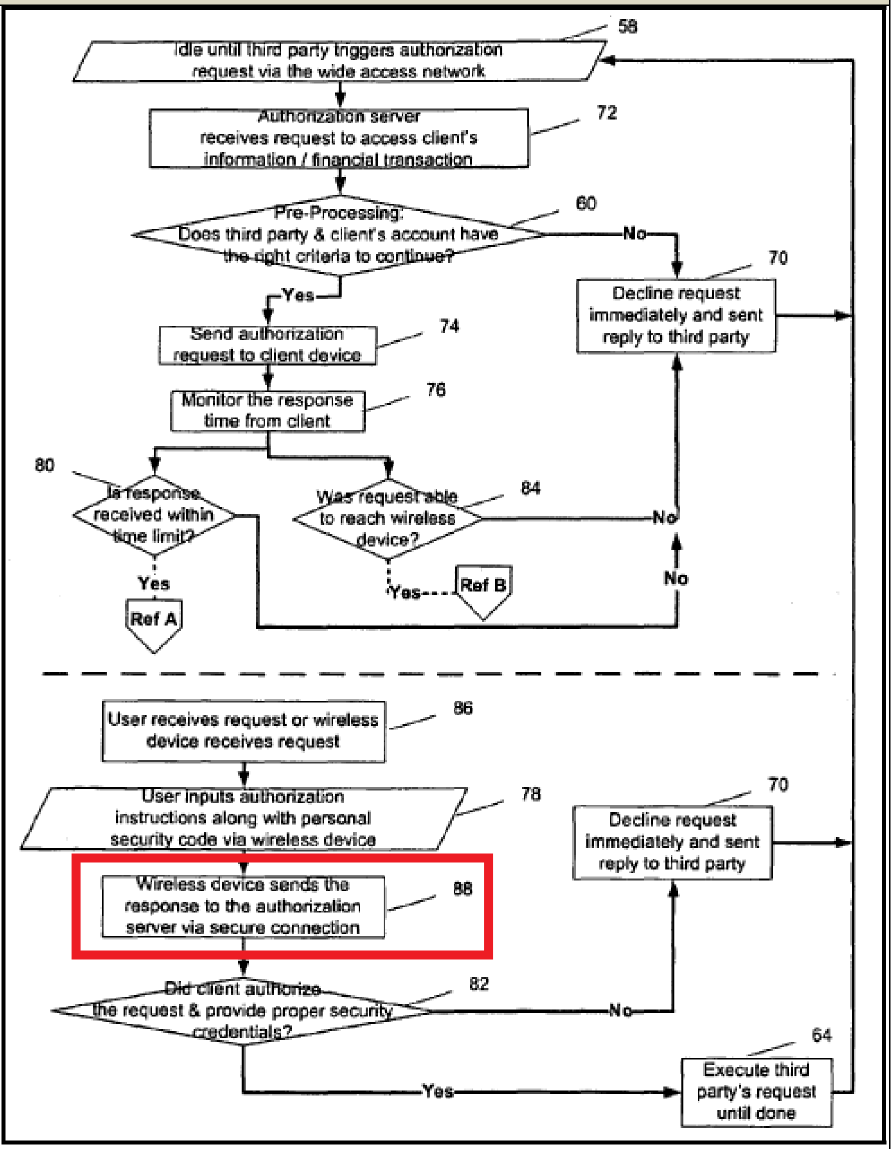
The ’648 Patent	**Law and Dua**
	wireless device is a mobile cellular phone, … such as ***a smart-phone***.”); *Id.* at ¶63 (“Upon receiving the request, the wireless device 38 will notify the user and automatically display the request for the user. ***The user will have the opportunity to input the response through the wireless device*** and be able to provide a PIN or personal digital signature (Block 78).”).
i) display on said I/O device an incoming identity verification request (IVR) sent to said user communications device by the verifier-computer through said verifier communications device;	**Law discloses that the user-computer is adapted to display on the I/O device an incoming IVR (e.g., text message) sent to the user communications device (“wireless device”) by the verifier-computer (“authorization server”) through the verifier communications device (“wireless gateway 30”).** Law, ¶49 (“***The request will travel through an encrypted secure channel connecting the authorization server and the user’s wireless device*** … Upon receiving the request, the wireless device will notify the user and automatically ***display the request*** for the user. A message similar to ‘company X requests action Y for an amount of Z, would you like to proceed?’ would be displayed on the wireless device. ”); *Id.* at ¶40 (“The ***wireless gateway 30*** is an entity that bridges the authorization server with the wireless network.”); Fig. 4:

The '648 Patent	**Law and Dua**
	 Idle until third party triggers authorization request via the wide access network 58 Authorization server receives request to access client's information / financial transaction 72 Pre-Processing: Does third party & client's account have the right criteria to continue? 60 No Decline request immediately and sent reply to third party 70 Yes Send authorization request to client device 74 Monitor the response time from client 76 80 Is response received within time limit? Was request able to reach wireless device? 84 No Yes Ref A Yes Ref B No User receives request or wireless device receives request 86 User inputs authorization instructions along with personal security code via wireless device 78 Decline request immediately and sent reply to third party 70 Wireless device sends the response to the authorization server via secure connection 88 Did client authorize the request & provide proper security credentials? 82 No 64 Execute third party's request until done Yes FIG. 4 **Fig. 1 shows that the request travels through the wireless gateway 30 to get to user communication devices 38.** Fig. 1:

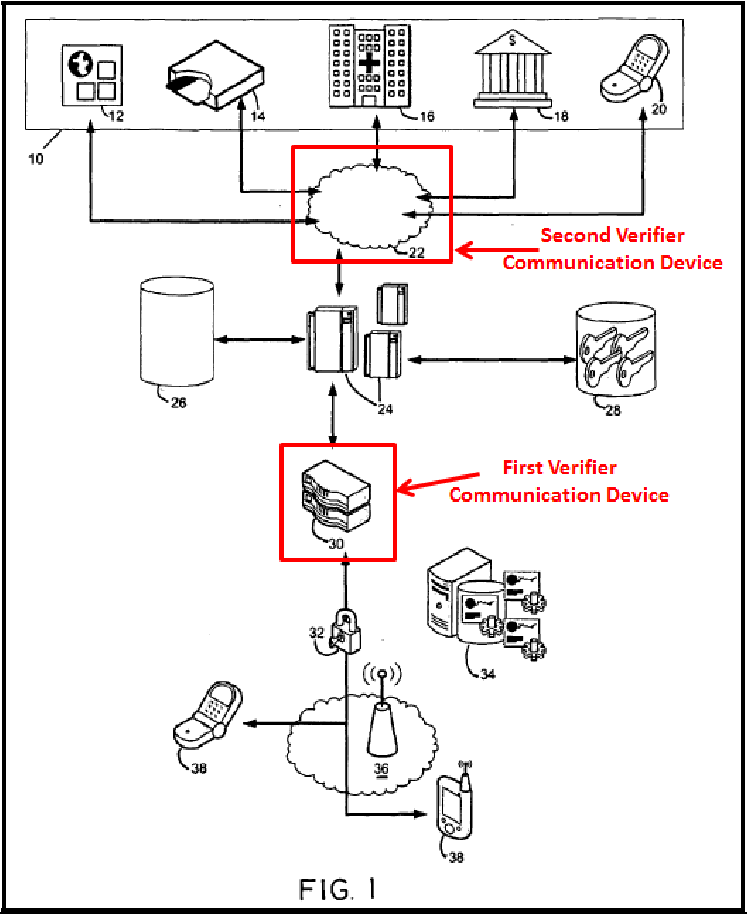
The ’648 Patent	**Law and Dua**
	 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 38 FIG. 1
ii) acquire the user’s input to said I/O device, wherein the user's input includes a putative secure identifier; and,	**Law discloses that the user-computer is adapted to acquire the user’s input to the I/O device, and the user’s input includes a putative secure identifier (“PIN or personal digital signature” as input by the user).** Law ¶49 (***“The user will have the opportunity to input the response through the wireless device and be able to provide a PIN or personal digital signature*** (Block 78).”). Fig. 4:

The '648 Patent	**Law and Dua**
	 Idle until third party triggers authorization request via the wide access network 58 Authorization server receives request to access client's information / financial transaction 72 Pre-Processing: Does third party & client's account have the right criteria to continue? 60 No 70 Decline request immediately and sent reply to third party Yes Send authorization request to client device 74 Monitor the response time from client 76 80 Is response received within time limit? Was request able to reach wireless device? 84 No No Yes Ref A Yes Ref B User receives request or wireless device receives request 86 User inputs authorization instructions along with personal security code via wireless device 78 70 Decline request immediately and sent reply to third party Wireless device sends the response to the authorization server via secure connection 88 Did client authorize the request & provide proper security credentials? 82 No 64 Yes Execute third party's request until done
iii) send a response to the IVR from said user communications device to said first verifier communications device,	**Law discloses that the user-computer is adapted to send a response to the IVR from the user communications device to the first verifier communications device ("wireless gateway").** Law ¶49 (***"The PIN or digital signature along with the appropriate response parameters are sent back to the authorization server through an encrypted secure channel via the wireless network."***). **Fig. 1 shows that the request travels from user communication devices 38, through the wireless gateway 30, to authorization server 24.** Fig. 1:

The ’648 Patent	**Law and Dua**
	 $ 12 14 16 18 20 10 22 26 24 28 30 32 34 38 36 38 FIG. 1 Fig. 4:

The ’648 Patent	**Law and Dua**
	 58 Idle until third party triggers authorization request via the wide access network 72 Authorization server receives request to access client's information / financial transaction 60 Pre-Processing: Does third party & client's account have the right criteria to continue? No 70 Decline request immediately and sent reply to third party Yes 74 Send authorization request to client device 76 Monitor the response time from client 80 Is response received within time limit? Was request able to reach wireless device? 84 No Yes Ref A Yes Ref B No 86 User receives request or wireless device receives request 78 User inputs authorization instructions along with personal security code via wireless device 70 Decline request immediately and sent reply to third party Wireless device sends the response to the authorization server via secure connection 88 Did client authorize the request & provide proper security credentials? 82 No 64 Execute third party's request until done Yes
wherein at least one of said user-computer and said verifier-Computer is adapted to: iv) receive as a first input a bona fide secure identifier retrieved from said	**Law discloses the verifier-computer (the “authorization server”) is adapted to:** **iv) receive as a first input a bona fide secure identifier (e.g., “PIN”) retrieved from the verifier database (the “database”). Specifically, Law discloses “verify[ing] the security credentials of the user.” A POSITA at the time of the alleged invention would understand that this step requires retrieving the bona fide secure identifier from the verifier database, as it would be**

The ’648 Patent	**Law and Dua**
verifier-database; v) receive as a second input the putative secure identifier; and, vi) compare the first input with the second input; wherein the electronic transaction proceeds if the first input and second input match.	**impossible to otherwise perform this verification.** **v) receive as a second input the putative secure identifier (e.g., “PIN”). A POSITA at the time of the invention would understand that as a result of Block 88 the authorization server would receive the personal security code entered in Block 78 and sent in Block 88; and;** **vi) compare (“verify”) the first input with the second input (e.g., the two PINs). Law also discloses that the transaction proceeds if the two inputs (e.g., the two PINs) match (are “correct”).** Law ¶49 (“**The PIN** or digital signature along with the appropriate response parameters are **sent back to the authorization server** through an encrypted secure channel via the wireless network.”). *Id.* at ¶50 (“***Upon receiving the response from the wireless device, the authorization server 24 will check if the response was received within a specified timeout period (Block 80) and verify the security credentials of the user and the wireless device (Block 82)****….* If the correct security credentials are provided, the specified instructions within the user’s response will be executed by the authorization server. ***An appropriate response will be sent back to the third party to complete the transaction (Block 64)***”); *Id.* at ¶58-59; Fig. 1.
3. The system of claim 2 wherein said user communications device is a personal communications device.	**Law discloses using a personal communications device (e.g., “mobile cellular phone,” “PDA,” “smart-phone”).** Law, ¶41 (“Typically the **wireless device** is a mobile **cellular phone**....”)

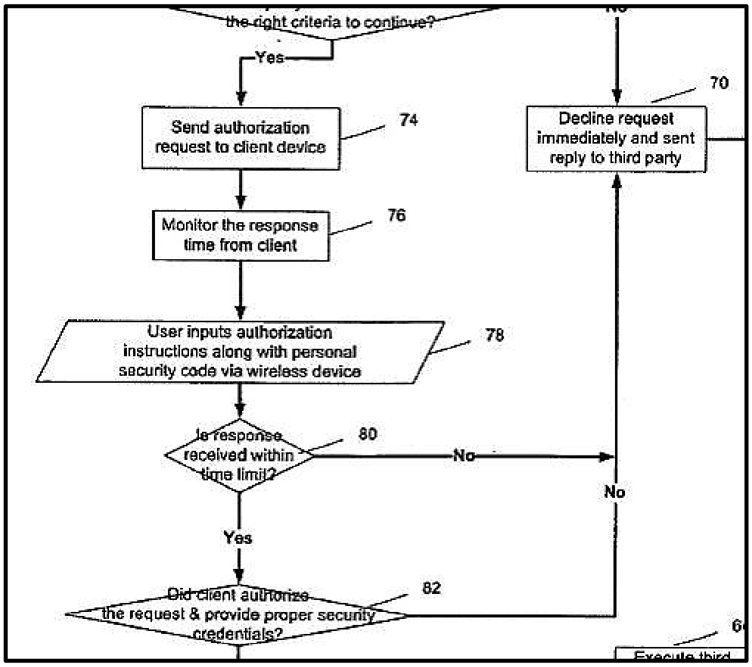
<u>**The ’648 Patent**</u>	<u>**Law and Dua**</u>
4. The system of claim 2 further comprising a second verifier communications device (803) for transmitting a confirmation output to a bank.	**Law discloses a second verifier communications device (“wide access network 22”) for transmitting a confirmation output to a bank (“third party entity 10”).** Law, ¶36 (“The purpose of the third party entity is to request an action that needs to be authorized by a user through their wireless device. ***For example,…[a]request will be initiated by the online merchant, sent through the credit card network 22 and into the authorization server 24 of the issuing bank.*** ”); <u>**Fig. 1 shows wireless gateway 30 (“first verifier connection device”) operatively connected to the wide access network 22 (“second verifier communication device”) via authorization server 24.**</u>  12 14 16 18 20 10 22 Second Verifier Communication Device 26 24 28 First Verifier Communication Device 30 32 34 38 36 38 FIG. 1

The ’648 Patent	**Law and Dua**
5. A user identity verification method for verifying the identity of a user by a verifier in the course of an electronic transaction, said user identity verification method comprising the steps of:	See Claim 1, Preamble.
(a) assigning a bona fide secure identifier to the user;	See Claim 1(a1).
(b) storing the bona fide secure identifier of Step (a) in a database that is accessible to the verifier;	See Claim 1(a2).
(c) storing a user access number for a user communications device in a database, wherein the database is accessible to the verifier, and wherein the user access number can be used to open a communications link with the user communications device;	See Claim 1(b).
(d) retrieving the user access number stored at Step (c);	See Claim 1(c).
(e) using the user access number retrieved at Step (d) to	See Claim 1(d).

The '648 Patent	**Law and Dua**
open a communications link between the verifier and the user communications device;	
(f) sending an identity verification request (IVR) from the verifier to the user through the communications link opened at Step (e);	See Claim 1(e).
(g) inputting by the user a putative secure identifier;	See Claim 1(f).
(h) receiving through the communications link opened at Step (e) a response to the IVR of Step (f);	See Claim 1(g).
(j) [sic] retrieving the bona fide secure identifier stored at Step (b); and,	See Claim 1(h).
(k) comparing the putative secure identifier input at Step (g) with the bona fide secure identifier retrieved at Step (j),	See Claim 1(i).
wherein the transaction proceeds if the comparison of Step (k) results in a match between the putative secure identifier and the bona fide secure identifier.	See Claim 1(j).

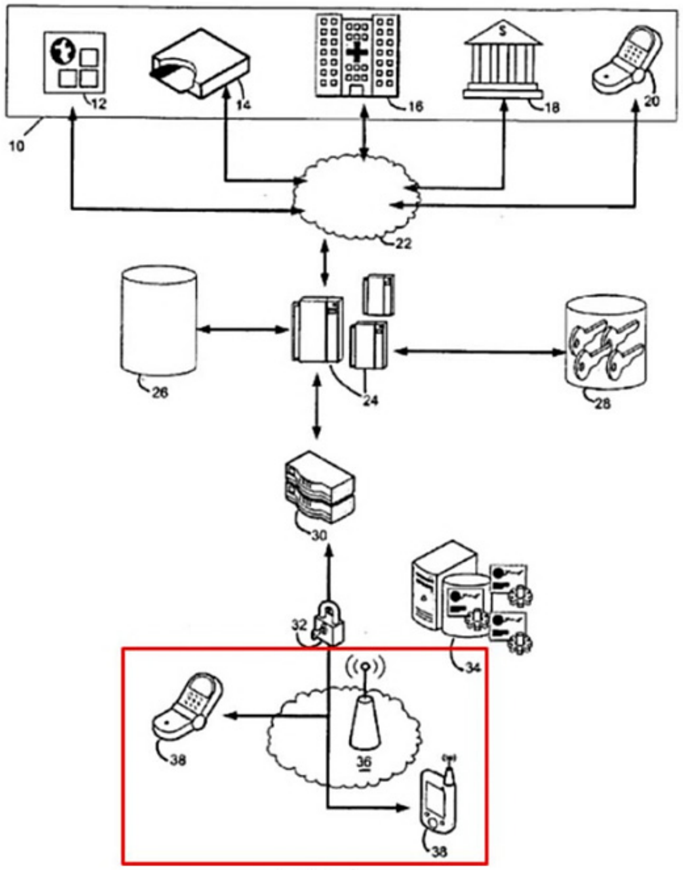
The ’648 Patent	**Law and Dua**
6. The method of claim 5 wherein the response received at Step (h) includes the putative secure identifier input at Step (g), and wherein Step (k) is performed by the verifier.	**Law discloses that the response received at Step (h) includes the putative secure identifier (the “PIN”) input at Step (g), and Step (k) (the comparison) is performed by the verifier (e.g., “issuing bank”).** Law, ¶49 (“The user will have the opportunity to input the response through the wireless device and be able to provide a PIN or personal digital signature (Block 78)... ***The PIN or digital signature along with the appropriate response parameters are sent back to the authorization server through an encrypted secure channel via the wireless network.***”); *Id.* at ¶50 (“Upon receiving ***the response*** from the wireless device, the ***authorization server 24*** will … ***verify the security credentials of the user and the wireless device*** (Block 82)…If the correct security credentials are provided, the specified instructions within the user’s response will be executed by the authorization server.”); *Id.* at ¶58-59.
7. The method of claim 5 further comprising the step of: (m) downloading local software to the user communications device.	**Law discloses software installed on a user communications device (“wireless device”).** Law ¶41 (“The wireless device must also be able to ***store an application*** that will process the request from the authorization server.”). *Id.* at ¶70 (“On the wireless device 38, ***proprietary software*** is used to send/receive messages to/from the authorization server.”). **Dua discloses downloading local software to a user communication device (“handset”) over the air. As stated above (See §VIII.B.3.b above), this was one of the well-known methods of installing software on wireless handsets at the time and a POSITA, at the**

The '648 Patent	**Law and Dua**
	time of the invention, would have been motivated to use it for convenience and flexibility in updating the software. Dua ¶199 ("[T]he mobile operator's Presence Service could initiate a request to a separate server that sends a message to the wireless end-user's handset, asking him if he would like to download the wallet application.... If the user agrees, ***the application can be provisioned on the user's device over-the-air.***").
8. The method of claim 7 wherein the IVR sent at Step (f) includes the bona fide secure identifier retrieved at Step (j), and wherein Step (k) is performed by the local software downloaded at Step (m), and wherein the response received at Step (h) includes the results of the comparison done at Step (k).	**Law discloses sending an IVR request and conducting the comparison ("verify") between the bona fide secure identifier and putative secure identifier to authorize the transaction. As discussed above, it would have been obvious to a POSITA to include the bona fide secure identifier retrieved at Step (j) in the IVR sent at Step (f). (Ex.1002, ¶65).** Law ¶49 ("However if no valid pre-authorization exists, ***the server will send out an authorization request to the user's wireless device (Block 74) and start monitoring the response time from the user (Block 76). The request will travel through an encrypted secure channel connecting the authorization server and the user's wireless device*** …. ***The PIN or digital signature along with the appropriate response parameters are sent back to the authorization server*** through an encrypted secure channel via the wireless network."); Law ¶50 ("Upon receiving the response from the wireless device, ***the authorization server 24 (the "verifier") will … verify the security credentials of the user and the wireless device*** (Block 82)."); Law ¶58 ("The user will have the opportunity to input the response through the wireless device 38 and be able to ***provide a PIN*** or personal digital signature (Block 78) as explained above. ***The PIN or digital signature along with***

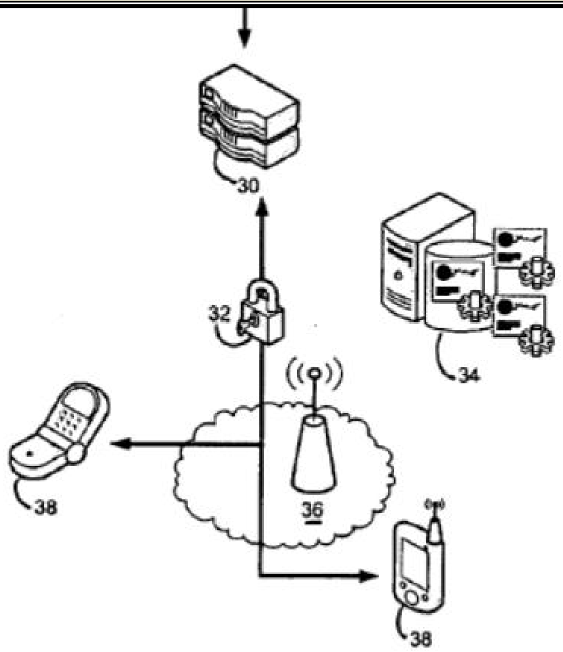
The ’648 Patent	**Law and Dua**
	the appropriate response parameters are sent back to the authorization server 24 through an encrypted secure channel via the secure wireless network 36.”); Law ¶59 (“Upon receiving the response from the wireless device 38, ***the authorization server (the “verifier”) will … verify the security credentials of the user*** and the wireless device (Block 82). FIG. 3:  the right criteria to continue? Yes No Send authorization request to client device 74 70 Decline request immediately and sent reply to third party Monitor the response time from client 76 User inputs authorization instructions along with personal security code via wireless device 78 Is response received within time limit? 80 No No Yes Did client authorize the request & provide proper security credentials? 82 6 Execute third **Dua teaches that a comparison between the bona fide secure identifier and putative secure identifier can be either conducted on the bank host computer system (at the verifier) and/or locally (on the wireless device) by the downloaded software (the “wallet application”).** Dua ¶366 (***“Data in the wallet application is encrypted and protected with a special wallet PIN code which is set by the wireless device owner during the setup of the application. The PIN is used to authenticate the user to the application***…**The default security setting in the**

The '648 Patent	**Law and Dua**
	wallet application is that PIN-entry is required before the wallet application can be "opened" and any credentials transmitted to an external device."); Dua ¶398 ("***Presently, with various bank card transactions, PINs are verified either online with a bank host computer system, or verified offline against security data onboard the card as in EMV "chip & PIN" transactions.***").
9. The method of claim 7 wherein the local software downloaded at Step (m) performs at least one of: (i) sending the response received at Step (h) and,(ii) Step (k).	**Law discloses that the software stored on user communication device send is the response received at Step (h).** Law ¶41 ("The wireless device must also be able to ***store an application*** that will ***process the request*** from the authorization server."); *Id.* at ¶70 ("On the wireless device 38, ***proprietary software*** is used to ***send/receive messages*** to/from the authorization server."); *Id.* at ¶49 ("***The PIN or digital signature along with the appropriate response parameters are sent back*** to the authorization server through an encrypted secure channel via the wireless network."). **Dua discloses downloading local software ("the wallet application").** Dua ¶199 ("… [T]he mobile operator's Presence Service could initiate a request to a separate server that sends a message to the wireless end-user's handset, ***asking him if he would like to download the wallet application...If the user agrees, the application can be provisioned on the user's device over-the-air.***").
10. The method	**Law discloses software stored on a user**

The '648 Patent	**Law and Dua**
of claim 7 wherein the local software downloaded at Step (m) performs the steps of: (n) receiving the IVR sent at Step (f); (o) formatting the IVR for display; and, (p) displaying the IVR formatted at Step (o) on an input/output (I/O) device of the user communications device.	**communications device ("wireless device") to receive the messages set forth in Step (f) as discussed with Claim 5. Law also teaches that the messages can be displayed as MMS messages, which are formatted for display. Separately, Fig. 1 shows the message being sent to different devices including the user communication device (the "wireless device") which requires that it be formatted for each device.** Law ¶40 ("Typically***, GPRS would be used for connection-oriented connections while short message service/enhanced message service/multimedia message service (SMS/EMS/MMS) would be used for connectionless communication.***"). *Id.* at ¶41 ("The wireless device must also be able to ***store an application t***hat will ***process the request*** from the authorization server."). *Id.* at ¶49 ("The request will travel through an encrypted secure channel connecting the authorization server and the user's wireless device … Upon receiving the request, the wireless device will notify the user and automatically ***display the request*** for the user."). *Id.* at ¶70 ("On the wireless device 38, ***proprietary software*** is used to ***send/receive messages*** to/from the authorization server."). Fig. 1:

The ’648 Patent	**Law and Dua**
	 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 38 FIG. 1 **Dua discloses downloading local software (“the wallet application”) “over-the-air.”** Dua ¶199 (“… [T]he mobile operator’s Presence Service could initiate a request to a separate server that sends a message to the wireless end-user's handset, ***asking him if he would like to download the wallet application in order to receive credentials from different issuers such as the one that tried to communicate with his wireless device. If the user agrees, the application can be provisioned on the user’s device over-the-air.***”).
11. The method of claim 7 wherein the	**Law discloses software stored on a user communications device (“wireless device”), can**

The ’648 Patent	**Law and Dua**
local software downloaded at Step (m) performs at least one of: (i) decrypting information received by the user communications device, and (ii) encrypting information sent by the user communications device.	**encrypt and decrypt information sent by the communication device.** Law ¶39 (“The authorization server 24 includes a database 26 which stores the account information of the users they serve. The authorization server will also include the secure storage 28 of encryption keys and/or certificates used to create a secure connection with the wireless devices.”). *Id.* at ¶41 (“The wireless device must also be able to ***store an application*** that will ***process the request*** from the authorization server***. This wireless application will be responsible for setting up the secure connection 32, securely storing certificates/encryption keys, displaying the request, accepting and creating the response.***”). *Id.* at ¶67 (“***In using a public key encryption scheme such as Transport Layer Security (TLS)***, the symmetric–key mentioned in the previous section can be used as a device password (Device key).”). *Id.* at ¶70 (“On the wireless device 38, ***proprietary software*** is used to ***send/receive messages*** to/from the authorization server.”). Fig. 1:

The '648 Patent	**Law and Dua**
	 FIG. 1 **Dua discloses downloading local software ("the wallet application") over the air. Dua also teaches that the downloaded software ("the wallet application") can be used to decrypt information.** Dua ¶199 ("… [T]he mobile operator's Presence Service could initiate a request to a separate server that sends a message to the wireless end-user's handset, ***asking him if he would like to download the wallet application in order to receive credentials from different issuers such as the one that tried to communicate with his wireless device. If the user agrees, the application can be provisioned on the user's device over-the-air.***"). *Id.* at ¶356 ("As such, an encrypted key could be transmitted from the reader to the wireless device, and ***decrypted by the wallet application on the wireless device using a decryption key*** that was previously sent by the credential issuer during issuance or through some other process.").

The '648 Patent	**Law and Dua**
12. The method of claim 5 wherein at least one of the IVR of Step (f) and the response received at Step (h) are encrypted when sent.	**Law discloses that the IVR ("request") and response ("PIN or digital signature") are encrypted when sent.** Law, ¶49 ("***The request will travel through an encrypted secure channel connecting the authorization server and the user's wireless device.*** ….The user will have the opportunity to input the response through the wireless device and be able to provide a PIN or personal digital signature (Block 78)… ***The PIN or digital signature along with the appropriate response parameters are sent back to the authorization server through an encrypted secure channel via the wireless network.***").
13. The method of claim 5 further including authorizing the transaction, said authorizing comprising the steps of: (q) sending a transaction authorization request to the user communications device; (r) receiving a response to the transaction authorization request of Step (q); and, (s) allowing the transaction to proceed only if the response received at Step (r) is to authorize the transaction.	**Law discloses sending a transaction authorization request ("an authorization request") to the user ("the user's wireless device"); receiving a response to the transaction server authorization request; and allowing the transaction to proceed only if the response received is to authorize the transaction.** **As discussed above (See Ex.1002, ¶70), Law discloses a single message that performs identity verification (as required by Claim 5) and transaction authorization (as required by Claim 13). Thus, the limitations of Claim 13 are taught by Law.** **In addition, to the extent the Patent Owner argues that this claim requires sending a separate message to authorize the transaction, it would have been obvious to a POSITA to utilize a separate message for transaction authorization, which is taught by Dua. (*See* Ex.1002, ¶71-72).** **Step (q): sending a transaction authorization request to the user communications device.** Law, ¶49 ("However ***if no valid pre-authorization exists, the server will send out an authorization request to the user's wireless device***.... The request will **travel through**

The '648 Patent	**Law and Dua**
	an encrypted secure channel connecting the authorization server and the user's wireless device.…"). **Step (r): receiving a response to the transaction authorization request of Step(q):** Law, ¶49 ("…Upon receiving the request, the wireless device will notify the user and automatically display the request for the user. ***A message similar to 'company X requests action Y for an amount Z, would you like to proceed?' would be displayed on the wireless device. The user will have the opportunity to input the response through the wireless device and be able to provide a PIN or personal digital signature*** (Block 78)…"); Law, ¶50 ("***Upon receiving the response from the wireless device, the authorization server will*** check if the response was received within a specified timeout period (Block 80) and ***verify the security credentials of the user and the wireless device*** (Block 82).…"). **Step (s): allowing the transaction to proceed only if the response received at Step (r) is to authorize the transaction.** Law, ¶50 ("***If the correct security credentials are provided, the specified instructions within the user's response will be executed by the authorization server.***").
14. The method of claim 13 further comprising the step of: (t) setting a flag in a database record, wherein the flag is associated with an account of the user and wherein the flag indicates whether or	**Dua discloses using a flag on a database record to indicate whether or not a transaction should proceed to the next step (as called for by Step (s)).** **A POSITA at the time of the invention would know that a flag (which is a common method of conveying status information in a database) could be used in a database to indicate where Steps (q) through (s) should be performed, e.g., in view of the account information.**

The ’648 Patent	**Law and Dua**
not at least one of Steps (q) through (s) are to be performed with respect to that account.	Dua, ¶417 (“… ***As such, a flag in the credit card customer account record signals to the credit card management system that an authorization approval can not be sent back to the retailer POS until an Over-the-Air PIN verification is completed.***”). **Law discloses checking the user’s account information for information such as sufficient funds in the account or the possibility of non-fraudulent activities. It would have been obvious to a POSITA at the time of the alleged invention to check for a user authorization flag before or after performing the checks described by Law.** Law, ¶45 (“When the third party initiates a transaction request (Block 58) through a wide access network … to the authorization server, then the ***authorization server*** pre-processes the request to ***determine*** if it has the right criteria (Block 60). ***In the case of credit card authorization, the criteria could include validity of the credit card number, sufficient funds in the account, and possibility of non-fraudulent activities. If all the criteria are satisfied, the authorization server will retrieve the pre-authorized information and determine if the request and the pre-authorized instructions match*** (Block 62).”).
15. The method of claim 5 further comprising the step of: (u) setting a flag in a database record, wherein the flag is associated with an account of the user and wherein the flag indicates whether or not transaction	**Dua discloses using a flag on a database record to indicate whether or not a transaction authorization is to be performed.** **A POSITA would know that a flag (which is a common method of conveying status information in a database) could be used in a database to indicate whether or not the transaction should be performed, e.g., in view of the account information.** Dua, ¶417 (“***As such, a flag in the credit card customer***

<u>The '648 Patent</u>	<u>Law and Dua</u>
authorization is to be performed.	***account record signals to the credit card management system that an authorization approval can not be sent back to the retailer POS until an Over-the-Air PIN verification is completed.***"). **Law discloses checking the user's account information for information such as sufficient funds in the account or the possibility of non-fraudulent activities. Thus, it would have been obvious to a POSITA to check the user's account for a flag indicating whether or not the user's identification should be verified.** Law, ¶45 ("When the third party initiates a transaction request (Block 58) through a wide access network … to the authorization server, then the **authorization server** pre-processes the request to **determine** if it has the right criteria (Block 60). **In the case of credit card authorization, the criteria could include validity of the credit card number, sufficient funds in the account, and possibility of non-fraudulent activities. If all the criteria are satisfied, the authorization server will retrieve the pre-authorized information and determine if the request and the pre-authorized instructions match** (Block 62).”).
19. The method of claim 5 further comprising the steps of: (dd) storing a device identifier of the user communications device of Step (c) in a database that is accessible to the verifier,	**Law further discloses the steps of:** **(dd) storing ("store" or "maintain the current list") a device identifier ("global unique identifier (GUID)") of the user communications device ("wireless device") in a database that is accessible to the verifier ("issuing bank");** Law ¶39 ("The authorization server 24 includes a database 26 which stores the account information of the users they serve. The authorization server will also include the secure ***storage 28 of encryption keys and/or certificates*** used to create a secure connection with the

The '648 Patent	**Law and Dua**
(ee) retrieving the device identifier stored at Step (dd); (ff) obtaining the device identifier of the user communications device of Step (e); and, (gg) comparing the device identifier retrieved at Step (ee) with the device identifier obtained at Step (ff); wherein the transaction is allowed to proceed only if the comparison of Step (gg) results in a match between the device identifier retrieved at Step (ee) and the device identifier obtained at Step (ff).	wireless devices. Depending on which authorization model used, the ***server must also keep track of the global unique identifier (GUID)*** of the wireless device in order to be able to contact it."). **(ee) retrieving the device identifier ("GUID");** **(ff) obtaining the device identifier of the user communications device;** Law ¶62 ("However, if no valid pre-authorization exists, the ***authorization server will look up the GUID of wireless device 38*** and attempt to connect to the wireless device with the GUID obtained (Block 94)."). *Id.* at ¶60 ("***Alternatively, another server can maintain the current list of active wireless devices and their identifiers.***"). **(gg) comparing ("verifying the security credentials") the stored device identifier with the device identifier of the user communication device;** *Id.* at ¶50 ("Upon receiving the response from the wireless device, the authorization server will check if the response was received within a specified timeout period (Block 80) and ***verify the security credentials of the user and the wireless device*** (Block 82)… . ***If the correct security credentials are provided, the specified instructions within the user's response will be executed by the authorization server.***"). **and allowing the transaction to proceed ("instructions within the user's response will be executed ") only if the comparison results in a match ("the correct security credentials are provided").** *Id.* at ¶67 ("In using a public key encryption scheme such

The ’648 Patent	**Law and Dua**
	as Transport Layer Security (TLS), ***the symmetric–key mentioned in the previous section can be used as a device password (Device key)*** … While the authentication server 24 can be authenticated via its own certificate using the public and private keys, the ***wireless device 38 should be authenticated with a password scheme if a client certificate is not available on the device***. Note that ***this is different from user authentication which takes place with the PIN***.”).

A. Ground 2: Claims 16-18 Are Unpatentable Under 35 U.S.C. §103(a) as Obvious Over Law and Dua in View of Salveson

1. The Disclosure of Salveson

Salveson, entitled “Electronic Transaction System,” discloses methods “[a]n all purpose transaction system using a universal card.” (Ex.1007, Abstract). Salveson issued on May 3, 2005 and is prior art under 35 U.S.C. §102(b).

Salveson recognizes that individuals often carry “a multitude of cards to perform their transactions and services in the economy,” including credit cards, bank cards, etc. (*Id.* at 1:14-27). Salveson further recognizes that carrying numerous cards around is inconvenient. (*Id.* at 1:27-37).

In response, Salveson discloses an “all-purpose consumer transaction system [that] allows a consumer to use one card (referred to herein as a ‘universal card’) for typical citizen/consumer transactions…” (*Id.* at 3:32-36). At the center of the disclosed system is a “universal card processing center (TCPC),” which processes the transactions for which the consumer uses the universal card. (*Id.* at 3:51-53).

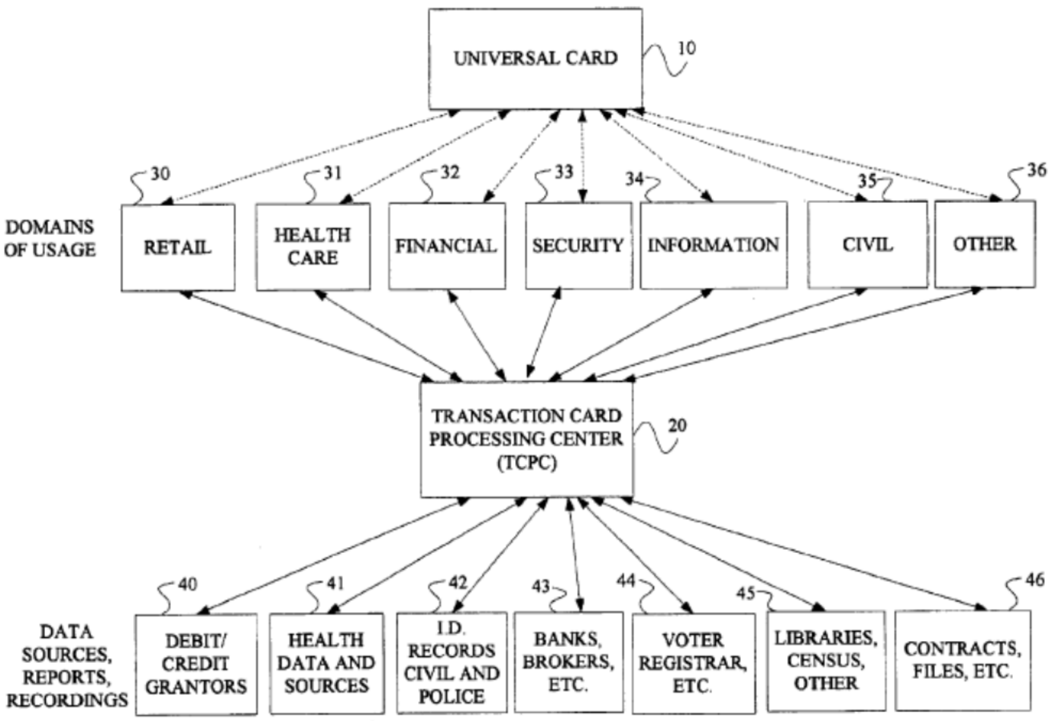


Fig. 1

As Figure 2 shows, information about the various vendors and cardholders is stored in databases located at the TCPC. (*Id.* at 6:12-23).

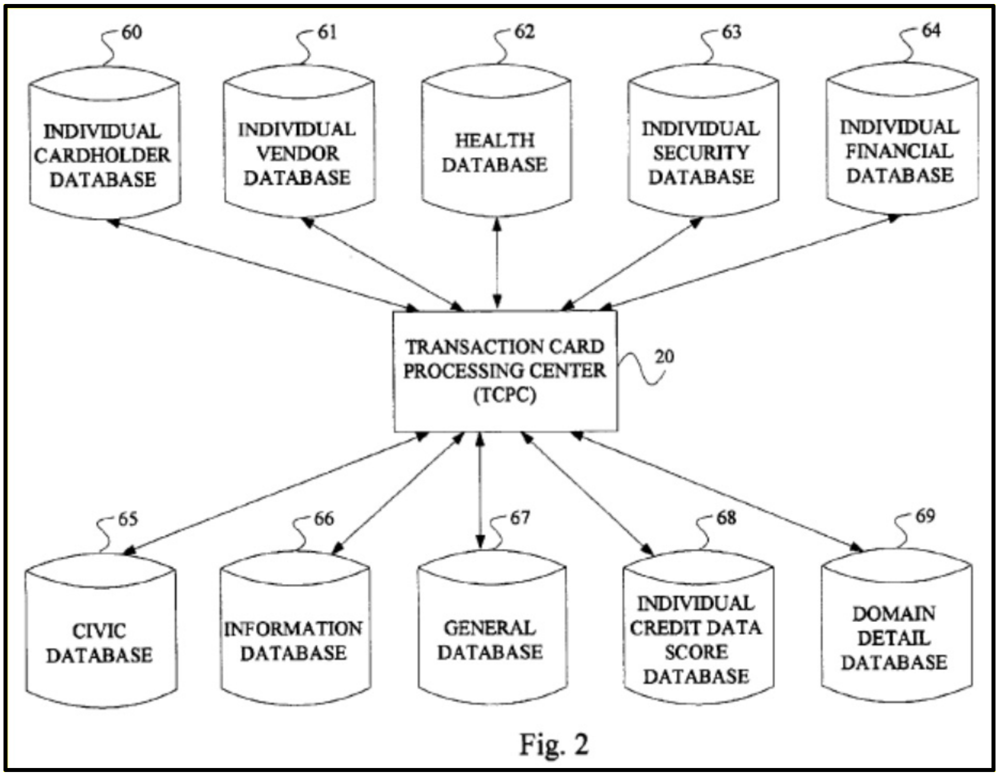

60
61
62
63
64
INDIVIDUAL CARDHOLDER DATABASE
INDIVIDUAL VENDOR DATABASE
HEALTH DATABASE
INDIVIDUAL SECURITY DATABASE
INDIVIDUAL FINANCIAL DATABASE
TRANSACTION CARD PROCESSING CENTER (TCPC)
20
65
66
67
68
69
CIVIC DATABASE
INFORMATION DATABASE
GENERAL DATABASE
INDIVIDUAL CREDIT DATA SCORE DATABASE
DOMAIN DETAIL DATABASE

Fig. 2

2. Obviousness of Claims 16-18 of the '648 Patent

It would have been obvious to a POSITA to combine the authorization methods of Law and Dua with the universal card of Salveson. The motivations for combining Law and Dua are discussed above (*See* Supra §VIII.B.3). In addition, Law, Dua and Salveson are all directed to electronic transaction processing, and thus, in the same field of endeavor. (Ex.1002, ¶83).

Law is concerned with, *inter alia*, avoiding the "theft, fraud and/or unauthorized us[e]" of credit cards, debit cards, etc. (Ex.1005, ¶13). Law, thus, proposes a secure authorization scheme which includes issuing authorization requests for individual transactions, and in which the card holder must authenticate by entering a personal identification number, in response to a request by an authorization server. (Ex.1002, ¶84).

Dua and Salveson are similarly concerned with the theft and loss of credit cards, and seek to avoid the associated difficulties by consolidating a customer's credit cards into a single device. Specifically, Dua discloses an "electronic wallet" that resides a on a wireless device. (Ex.1006, ¶18). The electronic wallet application takes the place of physical credit cards, and therefore limits the possibility of theft or loss. (Ex.1002, ¶85).

Salveson's solution to this same problem is to provide a universal card in which transaction processing can be performed through the universal card just as if the card holder were using his original charge card. (Ex.1002, ¶86). This method enables the transparency of security measures and issuance of authorization requests for individual transactions as if the card holder were using his original charge card. (*Id.* at ¶87).

A POSITA at the time of the alleged invention would recognize that the authentication system of Law and Dua would benefit from Salveson's universal card, which offers a solution to the problem of carrying multiple cards. (Ex.1002, ¶87). Under Supreme Court precedent, "any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the [prior art] elements in the manner claimed." *KSR*, 550 U.S. at 420. Here, the credit card fraud problem was addressed by Law (with an authentication scheme), Dua (with an electronic wallet) and Salveson (with a universal card). The transparent operation of Salveson's universal card in allowing transaction authorization is both compatible with and well-suited for combination with the additional security measures disclosed by Law and Dua. (Ex.1002, ¶87). Therefore, it would have been obvious to a POSITA to utilize the universal card of Salveson with the authentication scheme of Law and Dua to address the problem of credit card fraud. (Ex.1002, ¶87); *see also KSR*, 550 U.S. at 417 ("[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.").

Further, the universal card of Salveson was intended to improve credit card transactions by providing increased convenience. (Ex.1002, ¶88). A POSITA would have recognized that Salveson's universal card could be used to improve the authentication method of Law and Dua. (*Id.*). Moreover, a POSITA would have been able to readily combine the teachings of Law, Dua and Salveson, in the manner claimed to increase convenience. (*Id.*); *See also KSR,* 550 U.S. 415-16 ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.").

As shown in the Claim Charts below, Law, Dua and Salveson combine to teach all of the elements of Claims 16-18. As discussed, there was a clear motivation to combine the references and a POSITA would have had a reasonable expectation of success when making this combination. Thus, Claims 16-18 are obvious over the combined teachings of Law, Dua and Salveson. (Ex.1002, ¶89).

The ’648 Patent	**Law, Dua, and Salveson**
16. The method of claim 5 further comprising the steps of: (v) acquiring access information for an account of the user; and, (w) storing the account access information on a database that is accessible to the verifier.	**As discussed above, Law and Dua disclose every step of Claim 5.** **Salveson discloses the step of acquiring access information (“identification numbers and codes”) for an account of the user and storing the information on a database.** Salveson, 6:25-43 (“***The individual’s card database also includes a subfile for each merchant with whom the issuee has or has decided to have as an authorized vendor for him/her.*** Each subfile includes a summary of the issuee’s transactions, credit history and credit status with the vendor. ***The individual’s card database also includes a list of the identification numbers and codes of those vendors that serve the cardholder.***”); Fig. 2; *Id.* at 4:1-24 (“ ***For example, the cardholder may use the universal card 10 to access a funding card system, such as Visa®, MasterCard® or American Express® or to access a loan account, such as a loan at a credit union, a bank or a finance company***.”). **Law discloses storing account access information on a database that is accessible to the verifier (“issuer bank”).** Law ¶39 (“***The authorization server 24 includes a database 26 which stores the account information of the users they serve.***”);

The '648 Patent	**Law, Dua, and Salveson**
	Id. at ¶42 ("There are three authorization models that can be used by the user and their wireless device to ***allow a third party to access information*** …"); *Id.* at ¶45 ("When the third party initiates a transaction request… to the authorization server, then the authorization server pre-processes the request to determine if it has the right criteria (Block 60). ***In the case of credit card authorization, the criteria could include validity of the credit card number, sufficient funds in the account***, and possibility of non-fraudulent activities.").
17. The method of claim 16 further comprising the steps of: (x) issuing to the user a proxy transaction card containing data that can be used to authorize the verifier to access the account of Step (v); (y) using the data contained on the proxy transaction card to authorize the verifier to access the account of Step (v); (z) retrieving the account access information stored at Step (w); and, (aa) the verifier using the account access information retrieved at Step (z) to	**Law and Salveson, in combination, disclose steps (x) through (aa):** **Step (x): Salveson discloses issuing to the user a proxy transaction card ("universal card") containing data that can be used to authorize the verifier to access the account of Step (v);** **Step (y): Salveson discloses using the data contained on the proxy transaction card (an account number) to authorize the verifier to access the account of Step (v).** Salveson, 1:55-64 ("***The universal card allows a consumer/cardholder to conduct various types of transactions using a single card that has a single, unique, arbitrary identification number.***"); *Id.* at 9:3-20 ("***Once the card is swiped, the logic of FIG. 3 moves from a start block to block 100 where information is obtained from the swiped card.*** … ***If the card is a universal card 10, the information includes user (issuee) identification information, such as the cardholder's***

The '648 Patent	**Law, Dua, and Salveson**
access the account of Step (v) upon authorization at Step (y), wherein the transaction is made with respect to or debited to the account accessed at Step (aa).	***identification number.*** As is standard procedure, ***when the user swipes a card, the POS terminal display prompts the user for some type of verification, e.g., entry of a password or personal identification number (PIN)*** as exemplified in the POS display shown in FIG. 5."); Fig. 3. **Step (z): Law and Salveson disclose (z) retrieving the account access information stored at Step (w);** **Step (aa): Law discloses that the verifier uses the account access information retrieved at Step (z) to access the account of Step (v) upon authorization at Step (y), and, wherein the transaction is made with respect to or debited to the account accessed at Step (aa).** Law ¶39 ("***The authorization server 24 includes a database 26 which stores the account information of the users they serve.***"); *Id.* at ¶42 ("***There are three authorization models that can be used by the user and their wireless device to allow a third party to access information and or complete a financial transaction.***"); *Id.* at ¶45 ("... ***In the case of credit card authorization, the criteria could include validity of the credit card number, sufficient funds in the account, and possibility of non-fraudulent activities. If all the criteria are satisfied, the authorization server will retrieve the pre-authorized information and determine if the request and the pre-authorized instructions match*** (Block 62).").
18. The method of claim	**Law and Salveson combine to teach every**

The '648 Patent	**Law, Dua, and Salveson**
17, further comprising the steps of: (bb) displaying to the user at least one account the verifier is authorized to access; and, (cc) inputting by the user a choice as to which account displayed at Step (bb) the verifier is authorized to access.	**element of Claim 18.** **Step (bb): Law teaches that the user's wireless device can display certain information about the transaction regarding whether it should be allowed to proceed ("company X requests action Y for an amount of Z, would you like to proceed?").** Law, ¶49 ("Upon receiving the request, the wireless device will notify the user and automatically display the request for the user. A message similar to "**company X requests action Y for an amount of Z, would you like to proceed**?" would be displayed on the wireless device."). **Step (cc): Salveson teaches displaying to the user at least one account to be accessed, and the user inputting a choice as to which account should be accessed.** Salveson, 2:17-21 ("***A payment method (e.g., debit, credit card or vendor credit account) is selected by the cardholder. If there are multiple accounts available for the selected payment method, account identification is obtained from the card holder.***"); *Id.* at 9:21-28 ("***If the card being used for the transaction is a universal card 10, the cardholder will be asked for additional information (account type and account identification).***"); Figs. 3, 5-9.

IX. CONCLUSION

For the foregoing reasons, Petitioner has established a reasonable likelihood that it will prevail with respect to at least one of Claims 1-19 of the '648 Patent.

Therefore, this Petition should be granted, *Inter Partes* Review should be instituted, and Claims 1-19 should be found unpatentable and cancelled by the Board.

Respectfully submitted,

AMSTER, ROTHSTEIN & EBENSTEIN
LLP
Attorneys for Petitioner
90 Park Avenue
New York, NY 10016
(212)336-8000

Dated: January 18, 2017
New York, New York

By: /Charles R. Macedo/
Charles R. Macedo
Registration No.: 32,781

CERTIFICATE OF COMPLIANCE

Pursuant to 37 C.F.R. §42.24(d), I hereby certify that the foregoing PETITION FOR *INTER PARTES* REVIEW OF CLAIMS 1-19 OF U.S. PATENT NO. 8,285,648 contains 13,974 words, excluding the parts of the petition exempted by 37 C.F.R. §42.24(a), as measured by the word-processing system used to prepare this paper.

Dated: January 18, 2017 New York, New York	By: */Charles R. Macedo/* Charles R. Macedo Registration No.: 32,781 AMSTER, ROTHSTEIN & EBENSTEIN LLP 90 Park Avenue New York, NY 10016 (212) 336-8000

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§42.6(e) and 42.105, I hereby certify that on this 18th day of January 2017, a true copy of the foregoing PETITION FOR *INTER PARTES* REVIEW OF CLAIMS 1-19 OF U.S. PATENT NO. 8,285,648, together with Petitioner's Power of Attorney, Petitioner's Exhibit List, and Exhibit Nos. 1001-1011, was served via Priority Mail Express® on the patent owner at the following correspondence address of record for the subject patent:

DAN SCAMMELL
1729 Hampton Drive
Coquitlam, BC, CANADA V3E 3C9

In addition, service is also made at the following "address known to the petitioner as likely to effect service" pursuant to 37 C.F.R. §42.105(a):

VERMETTE & CO.
1177 West Hastings Street, Suite 320
Vancouver, BC, CANADA V6E 2K3

Anthony Cinotti
President and Director
VERIFY SMART CORP.
564 Wedge Lane
Fernley, NV 89408

Jean-Marc Zimmerman
ZIMMERMAN & PARAY LLP
233 Watchung Fork
Westfield, NJ 07090

Dated: January 18, 2017
New York, New York

By: */Charles R. Macedo/*
Charles R. Macedo
Registration No.: 32,781
AMSTER, ROTHSTEIN &
EBENSTEIN LLP
90 Park Avenue
New York, NY 10016
(212) 336-8000